Impact Telecommunicatiewet op online interactie

'Van opt-out naar opt-in'

Radboud Universiteit Nijmegen
Masterscriptie

31 december 2012

Naam:	**Niek Wolfkamp**
Opleiding:	**Informatiekunde/Information Sciences**
Begeleiders:	**Theo van der Weide (Radboud Universiteit Nijmegen)**
	Judith Matthijsse (SNS Bank)
Afstudeernummer:	**176 IK**

ABSTRACT

Tegenwoordig draait alles om gegevens. Persoonlijkheid via het internet is een opkomende trend. Hierbij is het gebruik van cookies een veelvoorkomende techniek. Hiermee kan de bezoeker service geboden worden waardoor de gebruikservaring toeneemt. Er werd steeds meer verzameld over bezoekers waardoor communicatie soms té persoonlijk werd en bepaalde organisaties konden hiermee inbreuk maken op de privacy van bezoekers. Om dit een halt toe te roepen is midden 2012 de Telecommunicatiewet gewijzigd in Nederland. Jarenlang konden organisaties via hun website veel cookies opslaan op de randapparatuur van bezoekers om zo enorme hoeveelheden gegevens te verzamelen. Hier lijkt nu een einde aan te komen. Voor sommige organisaties terecht, voor andere organisaties minder en brengt de gewijzigde wetgeving erg veel werk met zich mee. De website, de IT systemen, maar ook de bedrijfsvoering moet hierdoor mogelijk drastisch aangepast worden. Dit heeft een grote impact, niet alleen op de organisatie maar ook op de bezoeker. De gebruikerservaring zal veranderen. De online interactie gaat van een opt-out naar een opt-in met alle bijbehorende gevolgen. Deze scriptie geeft hier een eerste uiteenzetting over.

COLOFON

Titel:	Impact Telecommunicatiewet op online interactie
Ondertitel:	Van opt-out naar opt-in
Naam:	N.A. (Niek) Wolfkamp
Studentnummer:	0709409
Opleiding:	Informatiekunde/Information Sciences
Afstudeernummer:	176 IK
Plaats:	Nijmegen, Nederland
Datum:	31 december 2012

Radboud Universiteit Nijmegen

Universiteit:	Radboud Universiteit Nijmegen Onderwijsinstituut voor informatica en Informatiekunde Faculteit der Natuurwetenschappen, Wiskunde en informatica
Eerste begeleider:	prof. dr. ir. Th. P. (Theo) van der Weide
Tweede begeleider:	dr. L. (Luca) Consoli

SNS Bank

Organisatie:	SNS Bank N.V. Utrecht Onderdeel van SNS REAAL N.V. Interactie Marketing
Begeleiders:	J. (Judith) Matthijsse J. (Jurrien) Kamst

INHOUDSOPGAVE

1. Voorwoord 12
   1.1 SNS REAAL en SNS Bank 13
   1.2 Missie en visie 14
2. Het onderzoek 15
   2.1 Aanleiding en probleemstelling 15
   2.2 Verantwoording 17
   2.3 Theoretisch Kader 18
3. Eigenschappen van cookies 22
   3.1 Deelvraag 1: Wat zijn cookies en wat zijn de mogelijkheden hiervan? 22
      3.1.1 Technieken 25
      3.1.2 Eigenschappen van cookies 25
      3.1.3 Technische en niet-technische cookies 27
      3.1.4 Privacy 28
   3.2 Deelvraag 2: Waar worden cookies binnen SNS Bank voor gebruikt? 30
      3.2.1 Doeleinden 32
      3.2.2 Bedreigingen voor privacy 33
      3.2.3 Wijzigingen 35
4. Wetgeving voor gebruik van cookies 37
   4.1 Deelvraag 3: Wat zegt de eerdere wetgeving met betrekking tot het gebruik van cookies? 37
      4.1.1 Telecommunicatiewetgeving en Wbp 38
      4.1.2 Privacy- en cookiereglement 41
   4.2 Deelvraag 4: Wat zegt de gewijzigde wetgeving met betrekking tot het gebruik van cookies en hoe verschilt deze van de eerdere wetgeving? 42
      4.2.1 Voorbeelden 45
      4.2.2 Bereik van de wetgeving 46
      4.2.3 Omgekeerde bewijslast 47
5. Het cookie vraagstuk 49
   5.1 Deelvraag 5: Wat zijn de ontwikkelingen bij andere (financiële) organisaties en hoe gaan zij hier mee om? 49
      5.1.1 Europese Unie 51

5.1.2 Standaarden 52
5.1.3 Vier banken 53
5.1.4 De opties 54
5.2 Deelvraag 6: Waar dient de oplossing om de interactie tussen bank en bezoeker met cookies te ondersteunen aan te voldoen? 56
5.2.1 Vijf fasen plan 57
5.2.2 Tests 61
5.2.3 Requirements 62
5.2.4 Corporate en labels 65
5.3 Deelvraag 7: Welke aanpassingen dienen er gerealiseerd te worden binnen SNS Bank en welke invloed heeft dit? 66
5.3.1 Toestemming vragen en inloggen 66
5.3.2 De website 68
5.3.3 Opslag en gegevensverwerking 68
5.3.4 Bedrijfsvoering en soorten cookies 69
5.3.5 Overige aanpassingen 72
5.3.6 Ontwikkeling 72
6. Conclusie 73
6.1 Hoofdvraag 75
6.2 Toekomst 79
7. Bibliografie 81
8. Appendix 83
8.1 Details Cookies 83
8.2 Cookies indelen 84
8.3 Requirements 85

FIGUREN

Figuur 1.1 “Betrokken afdelingen binnen SNS Bank” 13
Figuur 2.1 “Onderdelen, belanghebbenden en eigenschappen” 16
Figuur 2.2 “Informatiekanalen bij contact” 17
Figuur 2.3 "Samenhang hoofdonderdelen in omgeving" 20
Figuur 2.4 “De omgeving met verschillende onderdelen en onderlinge samenhang” 21
Figuur 3.1 “Tweerichtingsverkeer met behulp van cookies” 22
Figuur 3.2 “Website bezoeken en handeling uitvoeren met of zonder cookie” 24
Figuur 3.3 “Cookies en kenmerkende eigenschappen” 26
Figuur 3.4 “Model van een cookie en eigenschappen.” 27
Figuur 3.5 “Soorten cookies en geldende wetgeving” 28
Figuur 3.6 “Cookies bij bezoek startpagina website SNS Bank” 30
Figuur 3.7 “Cookies bij bezoek webpagina SNS Bank Sparen” 31
Figuur 3.8 “Cookies bij bezoek webpagina SNS Bank Zakelijk” 31
Figuur 3.9 “Cookies ingedeeld op basis van kenmerkende eigenschappen” 32
Figuur 3.10 “Heldere gegevensverwerking met elke organisatie afzonderlijk” 34
Figuur 3.11 “Geen heldere verwerking van het soort gegevens met organisaties afzonderlijk” 35
Figuur 3.12 “Aantallen cookies tussen twee momentopnamen” 36
Figuur 4.1 “Tijdlijn met betrekking tot de wetgeving” 37
Figuur 4.2 “Gang van zaken bij gebruik van gegevens” 40
Figuur 4.3 “Situatie eerdere en gewijzigde wetgeving” 44
Figuur 4.4 “Bereik van de wetgeving” 47
Figuur 5.1 “Het ‘Cookie vraagstuk’” 49
Figuur 5.2 “Onderdelen waaraan voldaan dient te worden” 49
Figuur 5.3 “Opties ten behoeve van de gewijzigde wetgeving” 51
Figuur 5.4 “Informeren door vier Nederlandse banken” 54
Figuur 5.5 “Opties voor informeren en toestemming vragen” 55
Figuur 5.6 “Belanghebbenden use cases” 56
Figuur 5.7 “Vijf fasen voor aanpak toestemming vragen voor cookies” 57
Figuur 5.8 “De vier stappen gebaseerd op de leercyclus” 58

Figuur 5.9 “A/B testen” 61
Figuur 5.10 “Drie onderdelen waar verandering zal plaatsvinden” 66
Figuur 5.11 "Verhouding weergaven commerciële berichten aan klanten en bezoekers" 67
Figuur 5.12 "Verhouding doorklikpercentage van klanten en bezoekers" 67
Figuur 5.13 "Gegevens voor verwerking toestemming" 69
Figuur 5.14 “Koppeling bezoeker aan categorie met cookies voor verwerking toestemming” 69
Figuur 5.15 "Soorten cookies: doeleinden en consequenties bij uitschakeling" 71
Figuur 6.1 “Het verschil in wetgeving” 73
Figuur 6.2 “Meer nauwkeurigheid maar minder gegevens bij klanten ten opzichte van bezoekers” 74
Figuur 6.3 “Overzicht opties met voor- en nadelen” 75
Figuur 6.4 “De bezoeker ten opzichte van wetgeving, organisatie en techniek” 76
Figuur 6.5 “Van opt-out naar opt-in” 77
Figuur 6.6 “Benodigde aanpassingen” 77
Figuur 6.7 "Proces gebruikerservaring" 78
Figuur 6.8 “Gewijzigde wetgeving met nuance” 79

VERKLARENDE WOORDENLIJST

Aanbieder	Organisatie die de betreffende cookie plaatst.
App	Applicatie welke onder andere gebruikt kan worden op smartphones, tablets of andere randapparatuur.
Bewijslast	De manier waarop, en welke organisatie, het bewijs voor een bepaalde situatie moet aanleveren.
Bezoeker	Persoon die de website (het domein) bezoekt. Een bezoeker kan een klant zijn of dit worden. Ook wel aangeduid als gebruiker.
Cookie	Tekstbestand dat door een website via het internet naar de randapparatuur van een bezoeker gestuurd wordt en uitgelezen kan worden.
Domein	Het internetdomein dat de cookie plaatst en waar binnen de gegevensverzameling plaatsvindt.
First party cookie	Cookie die door de betreffende website (eigen domein) zelf geplaatst wordt.
Gebruiker	Persoon die gebruik maakt van een dienst of functionaliteit.
Gegevens	Data, waarden met een betekenis.
Inbound marketing	Interactie marketing waarbij het initiatief voor contact bij de bezoeker ligt, bijvoorbeeld gerichte aanbiedingen (via eigen domein).
Interactie marketing	Vorm van marketing binnen de organisatie om bezoekers en klanten te voorzien van persoonlijke service- en commerciële berichten.
Klant	Persoon die klant is van de organisatie en kan inloggen op de website (het domein). Ook wel aangeduid als gebruiker.
Klikgedrag	Gegevens van een bezoeker die verzameld worden op basis van het bezoek aan een website (waar klikt de bezoeker op). Ook wel surfgedrag genoemd.
Label	Onderdeel binnen de organisatie van SNS Reaal, bijvoorbeeld SNS Bank.
Outbound marketing	Interactie marketing waarbij het initiatief voor contact bij de organisatie ligt, bijvoorbeeld door opbellen of het sturen van een brief.
Opt-in	Het vooraf geven van toestemming alvorens een bepaalde handeling uitgevoerd wordt.
Opt-out	Het intrekken van toestemming als een bepaalde handeling al uitgevoerd wordt of uitgevoerd kan gaan worden.

Persoonsgegevens	Gegevens die terug zijn te herleiden tot een persoon en gegevens als naam, adres en/of telefoonnummer.
Privacy- en cookiereglement	Document op juridische basis over het gebruik van gegevens en cookies met toelichting.
Randapparatuur	Apparaten van de bezoeker of klant zoals een computer, laptop, tablet en telefoon.
Sessie	Periode van begin van een bezoek aan de website tot het einde van het bezoek.
Standaard	Een manier van handelen/communiceren op (vrijwel) uniforme wijze (binnen een bepaalde branche of niveau).
Technische cookie (functionele)	Cookie die zonder toestemming geplaatst mag worden om zo de dienstverlening mogelijk te maken en de website te laten functioneren. Ook wel aangeduid als functionele cookie.
Third party cookie	Cookie die door een andere aanbieder (buiten eigen domein) geplaatst wordt.
Toezichthouder	Overheidsorgaan dat de gang van zaken onderzoekt en bij onjuistheden met de juiste bewijsvoering ingrijpt.
Tracking cookie	Cookie die het surf-/klikgedrag van de bezoeker volgt en op basis hiervan een profiel opbouwt.
Wbp	Wet bescherming persoonsgegevens, wet ter bescherming van de verwerking van persoonsgegevens.
Wet/ Telecommunicatie-wetgeving	De wetgeving welke in gaat op het gebruik van technieken als cookies en de manier waarop dit dient te gebeuren.

1. VOORWOORD

In deze masterscriptie voor de studie Informatiekunde/Information Sciences aan de Radboud Universiteit te Nijmegen is de impact van de gewijzigde Telecommunicatiewet (ook wel 'Cookiewet') op online communicatie onderzocht. Door middel van verschillende hoofdstukken zal dit vraagstuk behandeld worden, zowel op abstract niveau als in de situatie van SNS Bank.

Het volgende hoofdstuk beschrijft het onderzoek van deze scriptie. Hierna wordt in hoofdstuk drie beschreven wat de eigenschappen en mogelijkheden van technieken als cookies zijn. Dit aan de hand van twee deelvragen. In hoofdstuk vier wordt de eerdere en nieuwe situatie op het gebied van de gewijzigde wetgeving uiteengezet. In hoofdstuk vijf is een voorstel gedaan over het gebruik van cookies en de benodigde toestemming. Dit gaat ook specifieker in op de situatie bij SNS Bank. Hierbij is onder andere een plan met meerdere fasen beschreven. Daarnaast zijn de benodigde aanpassingen uiteengezet.

Hoofdstuk zes bestaat uit de conclusie en beantwoording van de hoofdvraag. Ook worden er suggesties gegeven voor aanvullend onderzoek. Na de bibliografie zijn in de appendix de resultaten van verschillende onderdelen te raadplegen.

Zowel Judith Matthijsse en Jurrien Kamst (SNS Bank) als Theo van der Weide en Luca Consoli (Radboud Universiteit Nijmegen) hebben bijgedragen aan de begeleiding van deze scriptie. Graag wil ik hen bedanken voor de gegeven suggesties, feedback en hun kritische blik.

Ik wens u veel leesplezier,

Niek Wolfkamp

SNS REAAL/SNS Bank is actief in Nederland, de bedrijfscultuur en de voertaal zijn ook Nederlands. Deze scriptie is om deze redenen dan ook in het Nederlands geschreven.

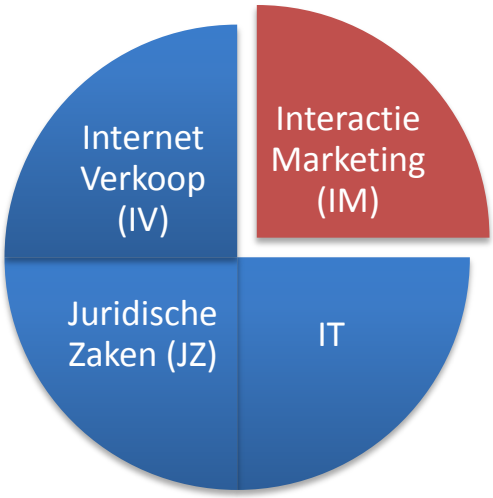
Openbare versie

Vanwege vertrouwelijkheid zijn sommige onderdelen niet beschikbaar in deze openbare versie. Interne informatie van SNS Bank is bij sommige onderdelen als bron of literatuur gebruikt. Tevens kunnen de verkregen gegevens op momentopnamen veranderen of deze zijn al veranderd.

1.1 SNS REAAL en SNS Bank

SNS REAAL[1] is één van de grote financiële dienstverleners in Nederland. De organisatie heeft diverse merken, te weten SNS Bank, REAAL, Zwitserleven en SNS Asset Management. Onder REAAL vallen Proteq, Route Mobiel en Zelf.nl. Naast SNS Bank (sinds 1817) zijn ook RegioBank, ASN Bank, BLG, SNS Securities en SNS Property Finance onderdelen van de organisatie.

Binnen meerdere merken wordt er gebruik gemaakt van cookies, het onderwerp van deze scriptie vanwege de veranderende wetgeving (1). Deze scriptie is gericht op het bank label, ofwel SNS Bank. Binnen de afdeling 'Interactie Marketing' zal het onderzoek plaatsvinden. De veranderende wetgeving heeft veel invloed op de gehele organisatie en meerdere afdelingen zijn hier dan ook bij betrokken (figuur 1.1). Belangrijk is dat de missie 'Eenvoud in geldzaken' voorop blijft staan (2), ofwel gebruikersgemak is zeer belangrijk.



Figuur 1.1 *"Betrokken afdelingen binnen SNS Bank"*

Zowel Internet Verkoop als Interactie Marketing zijn van belang aangezien zij respectievelijk de website en het inbound marketing systeem gebruiken en beheren. Juridische Zaken zal advies geven over de gewijzigde wetgeving en de knelpunten aangeven. IT zal in overleg de impact op de systemen bepalen en uiteindelijk de implementatie voor haar rekening nemen. De te varen koers op hoog niveau bepaalt de betreffende directie. Het resultaat dient te passen binnen de missie en visie.

[1] www.snsreaal.nl *(Laatst geraadpleegd op 31-12-2012)*

1.2 Missie en visie

Om te weten waarvoor SNS Bank staat is het van belang de missie en visie van de organisatie te beschrijven. SNS REAAL heeft 'Eenvoud in geldzaken' hoog in het vaandel staan: "Bij SNS Bank bepalen klanten zelf hoe, waar en wanneer ze hun geldzaken regelen. Via de website, aan de telefoon, met een adviseur aan huis of in een SNS Winkel. SNS Bank staat voor eenvoud in geldzaken. Zo toegankelijk mogelijk, zodat klanten weten waar ze financieel aan toe zijn."[2]

Gebaseerd op het jaarverslag (2) is zowel betrouwbaarheid als transparantie zeer belangrijk. Dit is van toepassing op alle contactmomenten en dus ook bij communicatie via de website. SNS Bank dient altijd toegankelijk te zijn voor iedereen. Dit wordt onder andere gefaciliteerd met SNS Winkels en bankieren met de mobiele telefoon of tablet. Ook is het behouden van het Waarmerk Drempelvrij[3] erg belangrijk. Mensen van iedere leeftijd en met beperkingen moeten hun bankzaken kunnen regelen. Duurzaamheid is tevens belangrijk en hetzelfde geldt voor veiligheid. Alle communicatie met SNS Bank dient veilig en betrouwbaar te zijn. Het interne manifest 'Mens voor mens' onderschrijft dit: Ieder mens wil op zijn eigen manier bankzaken regelen daarom wil SNS Bank de menselijke maat terugbrengen in geldzaken door de ontwikkeling van eenvoudige dienstverlening.

De veranderingen door de gewijzigde Telecommunicatiewet, het gebruik van technieken als cookies en de verplichting om toestemming te vragen aan de bezoeker moet binnen de missie en visie blijven passen.

[2] www.snsreaal.nl/merken/onze-merken/sns-bank-4.html *(Laatst geraadpleegd op 31-12-2012)*

[3] Waarmerk Drempelvrij is een Nederlands kwaliteitsmerk om in meerdere niveaus uit te drukken hoe toegankelijk een website is.

2. HET ONDERZOEK

Voor deze scriptie is het volgende onderzoeksplan opgesteld: de probleemstelling, verantwoording en het theoretisch kader zullen aan bod komen alvorens de technieken en de mogelijkheden hiervan beschreven worden.

2.1 Aanleiding en probleemstelling

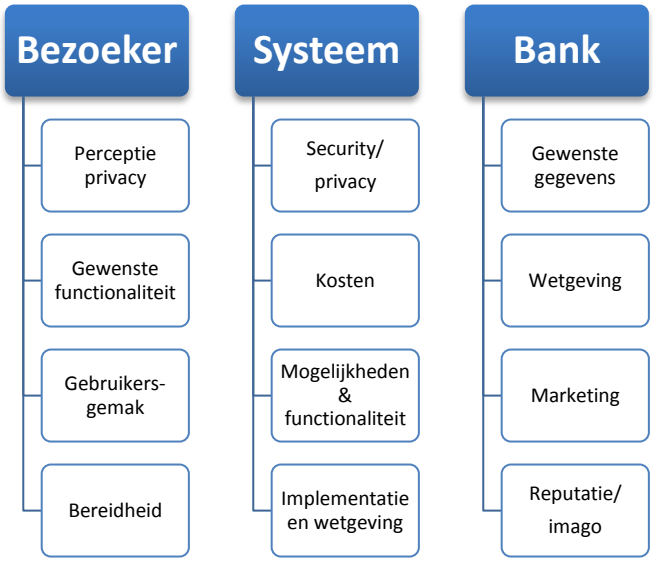
Tegenwoordig draait alles om informatie. In deze informatie consumerende maatschappij is het van belang dat dit zodanig gebeurt dat zowel de verstrekker als ontvanger hier profijt van hebben. Een grote schakel die dit mogelijk maakt is ICT. Grote hoeveelheden informatie kunnen hiermee met grote snelheid en ook zeer nauwkeurig verwerkt, verstuurd en ontvangen worden (3). Organisaties maken hier tegenwoordig veel gebruik van. Steeds meer informatievoorziening verloopt online en steeds meer offline communicatie raakt ondergeschikt of verdwijnt zelfs. Ook worden steeds vaker apparaten als smartphones en tablets gebruikt voor meer verschillende doeleinden. Hierdoor zal de techniek steeds meer verweven raken met het dagelijkse leven, de scheiding tussen de online en offline wereld vervaagt (4). Hierbij is de persoonlijke benadering een groeiend fenomeen waardoor steeds meer gegevens van personen verwerkt en gebruikt worden voor vele doeleinden.

Het verschilt per sector hoe dit verloopt en bij de één is meer zorgvuldigheid nodig dan bij de ander. Een situatie waar zorgvuldigheid van gegevens essentieel is, is de bankensector. De trend van online communicatie is hier al een tijd gaande. Bij alles dient veiligheid en correctheid voorop te staan: confidentiality, integrity en availability staan hoog in het vaandel. Ook accountability (ook wel traceerbaarheid) is van groot belang. Een andere factor die hier deels mee samenhangt is de reputatie van de bank, dit staat of valt met een goed informatiesysteem en betrouwbaarheid. Daarnaast moeten zowel de bank als klant/bezoeker er voordelen van hebben. Privacy is tevens een onderdeel wat van belang is, zowel feitelijk als in de perceptie van de bezoeker. De bezoeker is zich hier namelijk steeds meer van bewust maar tegelijkertijd bereid om privacy ‘in te ruilen’ voor meer gebruikersgemak. Dit wordt mede veroorzaakt door het gevoel van online anonimiteit (5) en een door te lopen leercyclus. Dit is in sommige gevallen een vals gevoel aangezien er technieken beschikbaar zijn welke personen ongemerkt online kunnen herkennen. De gewijzigde wetgeving heeft daarnaast als doel de privacy van de bezoeker te beschermen.

Momenteel beschikt SNS Bank over meerdere systemen waaronder het inbound marketing systeem. Door middel van cookies wordt een klant/bezoeker herkend en kan het klikgedrag verzameld worden. Hiermee is veel informatie over bezoekers voorhanden, ook kan dit gemakkelijk toegepast en geëvalueerd worden. Zowel gebruikersgemak aan de ene kant als security en privacy aan de andere kant zijn de belangrijkste pijlers hiervoor. Het meest geschikt is dan ook om een zodanige architectuur en functionaliteit te hanteren waar beide belanghebbenden voordeel van hebben. Het voordeel ligt voor de bezoeker of klant in gebruikersgemak en voor de organisatie in informatie voor service en marketing doeleinden. Voor beide belanghebbenden kan zo een persoonlijke benadering ingezet worden. Met de

veranderende Telecommunicatiewetgeving (1) (voortvloeiend uit de Europese wetgeving (6)) waarbij bezoekers toestemming moeten geven voor het plaatsen en uitlezen van gegevens (cookies) op hun apparaten (opt-in) ligt hier een erg grote uitdaging. Hoe laat je een bezoeker inzien dat het een ondersteuning van het gebruikersgemak kan zijn en niet in alle gevallen een aanval op hun privacy zal betekenen? Hoe dient de huidige situatie aangepast te worden om te voldoen aan deze gewijzigde wetgeving? Welke invloed zal dit hebben op de belanghebbenden en hun perceptie? Hoe ziet de situatie eruit waarin een opt-in gehanteerd dient te worden in plaats van een opt-out zoals voor de wetswijziging het geval was?

Om dit grondig te bewerkstelligen zijn enkele stappen nodig om vervolgens requirements op te kunnen stellen. Hoe past het binnen de huidige maatschappij en hoe binnen de voor handen zijnde ICT? Hoe kan de perceptie van de bezoeker veranderen, evenals de reputatie van de organisatie? Welke afweging tussen gebruikersgemak en security/privacy dient en kan er gemaakt worden? Dit alles is een interessant vraagstuk waarvan de uitkomst zeer verhelderend is voor SNS Bank bij het blijven gebruiken en verbeteren van de huidige systemen, waaronder inbound marketing. Figuur 2.1 geeft een beknopt overzicht van de drie grootste onderdelen met enkele noemenswaardige punten, bij elk onderdeel is nog uitbreiding mogelijk. Zo kan informatie uit het inbound marketing systeem ook gebruikt worden voor gerichte outbound marketing, dit gebeurt echter niet online maar zal wel een toekomstige ontwikkeling kunnen zijn.

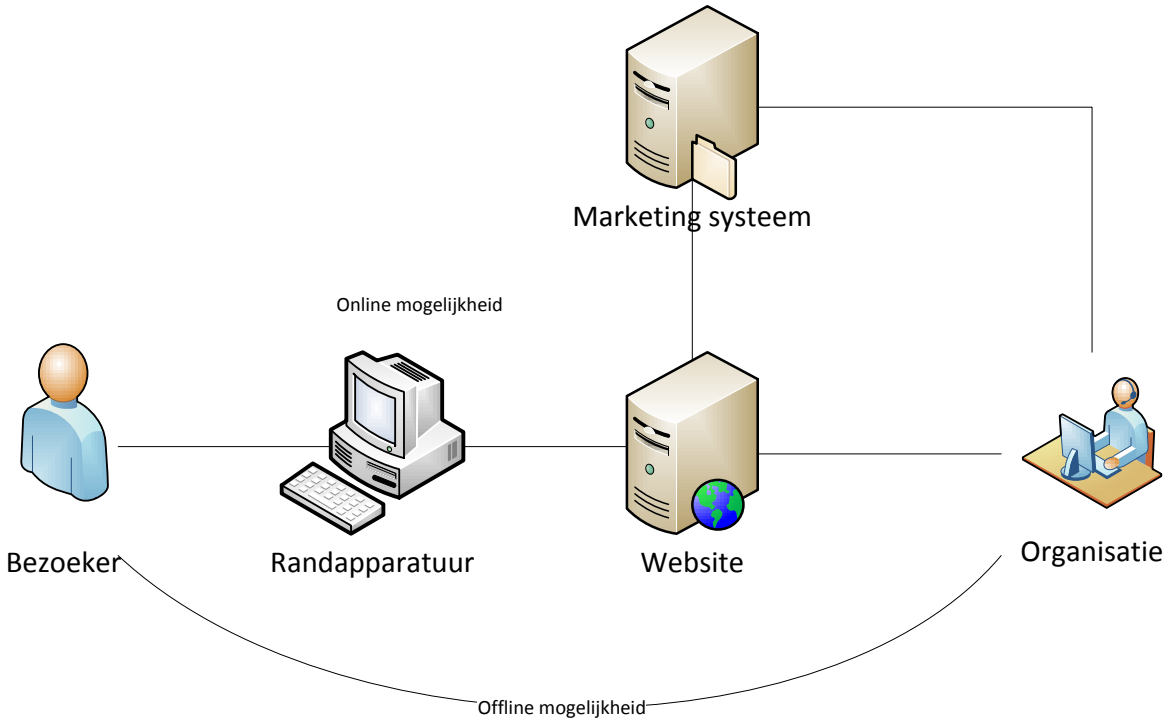


Figuur 2.1 *"Onderdelen, belanghebbenden en eigenschappen"*

Daarnaast zijn er nog meer partijen van belang (of kunnen dit zijn), welke dit zijn zal onderzocht moeten worden. Het is te stellen dat het gehele proces zich in een cycle bevind. Hier dient rekening mee te worden gehouden. Ook zal de bezoeker bij handelingen zijn perceptie met betrekking tot gebruikersgemak, privacy en de organisatie blijven aanpassen. Hij zal dit ook vergelijken met gelijksoortige handelingen in het offline leven ten opzichte van de online handeling die hij uitvoert

(figuur 2.2) (4). Dit schematische figuur geeft tevens een overzicht van globale informatiekanalen. De bezoeker heeft meer controle en inzicht in de offline mogelijkheid dan in de online mogelijkheid vanwege het feit dat er minder tussenliggende systemen en technieken, zoals cookies, gebruikt kunnen worden.

Het is duidelijk dat de omgeving met onderdelen en belanghebbenden erg complex is. De processen tussen de bezoeker, het systeem en de bank dienen geconcretiseerd te worden waarin het gebruik van essentiële of additionele informatie (verzameld via technieken als cookies) duidelijk zichtbaar is. Zodoende kunnen de requirements, waarbij zowel de bezoeker als de bank zoveel mogelijk voordeel heeft, worden opgesteld. Een doordachte en functionele aanpak moet geheel voldoen aan de gewijzigde wetgeving en passen in de huidige maatschappij.



Figuur 2.2 *"Informatiekanalen bij contact"*

2.2 Verantwoording

Gesteld kan worden dat de punten besproken in de 'Aanleiding en probleemstelling' als doel hebben om requirements en richtlijnen op te stellen voor SNS Bank, om zo een bank te blijven waarvan de doelstellingen blijven bestaan (2), voorbereid te zijn op toekomstige ontwikkelingen, zal blijven groeien qua mogelijkheden en klantaantallen en ICT zo doeltreffend mogelijk in kan zetten. Zowel gezien vanuit SNS Bank als vanuit de bezoeker. Met de gewijzigde wetgeving voor het gebruik van technieken als

cookies (1) krijgen heel veel organisaties maar ook bezoekers te maken met de gevolgen hiervan. SNS Bank maakt veelvuldig gebruik van cookies en zal dus ook aanpassingen moeten implementeren.

De resultaten zullen voor de specifieke situatie binnen SNS Bank waardevolle en bruikbare informatie opleveren. De hoofdlijnen kunnen echter ook van belang zijn voor veel meer organisaties die met de wetswijziging te maken hebben, en tevens voor iedere website bezoeker. Dit is momenteel specifiek voor de situatie in Nederland maar gezien de Europese wetgeving (6) die constant in beweging is kan dit voor organisaties binnen de Europese Unie ook interessante inzichten opleveren, zeker wanneer zij actief zijn in Nederland. Iedere organisatie of website die standaard gebruik maakt van cookies zal moeten inspelen op de gewijzigde wetgeving. Momenteel is er nog weinig bekend over de veranderende situatie en de impact daarvan. Deze scriptie zal hier een uiteenzetting voor geven met requirements voor een mogelijke oplossing.

2.3 Theoretisch Kader

Centraal staat het gebruik van online communicatie, de perceptie van de bezoeker en de (veranderende) wetgeving. De in de 'Aanleiding' vermelde aspecten en vragen zullen onderzocht en beantwoord worden. Hoofdlijnen van de scriptie zijn:

- In kaart brengen wat cookies precies zijn en waarvoor deze bij SNS Bank gebruikt worden. Hierbij zullen gegevens geanalyseerd worden aan de hand van de doeleinden voor gebruik. Dit is zowel van belang voor de inbound marketing maar bijvoorbeeld ook voor externe advertenties. Hierbij is er een samenwerking met de verschillende afdelingen.
- Het analyseren van de huidige Telecommunicatiewet en wetgeving voor technieken als cookies, de gewijzigde wetgeving en de onderlinge verschillen. Hierop gebaseerd is te bepalen welke veranderingen doorgevoerd dienen te worden om te voldoen aan de gewijzigde wetgeving en de wijze waarop dit mogelijk is in de specifieke situatie.
- Hoe het systeem met de gewijzigde wetgeving zo goed mogelijk binnen de specifieke situatie kan functioneren en ook de bezoeker in de gebruikerservaring tevreden te stellen. Hierdoor kunnen de missie en visie van SNS Bank gewaarborgd blijven.
- Onderzoeken op welke wijze het gebruik van online communicatie gewijzigd dient te worden. Op basis hiervan kunnen requirements voor verandering en adviezen opgesteld worden voor een mogelijke oplossing voor SNS Bank.

Om deze punten correct te kunnen onderzoeken is het van belang voorafgaand aan het onderzoek enkele begrippen duidelijk te stellen. De volgende begrippen (gebaseerd op (4)) spelen een belangrijke rol:

- **Wetgeving:**
  De geldende wetten en regels in een land of lidstaat. In dit geval gaat het om de Telecommunicatiewetgeving in Nederland (1) gebaseerd op die van de Europese Unie (6) voor haar lidstaten waar ook Nederland tot behoort. Wetgeving zorgt ervoor dat zaken of handelingen op een bepaalde manier dienen te verlopen. Overtreding kan dan ook bestraft

worden door justitie of een toezichthouder (bij de handhaving van de Telecommunicatiewetgeving is dit de OPTA[4]). In Nederland is er ook de Wet bescherming persoonsgegeven (Wbp). Deze wet gaat in op de verwerking van persoonsgegevens en de privacy van een bezoeker. In de gewijzigde wetgeving zal hierbij de zogenoemde omgekeerde bewijslast in werking treden.

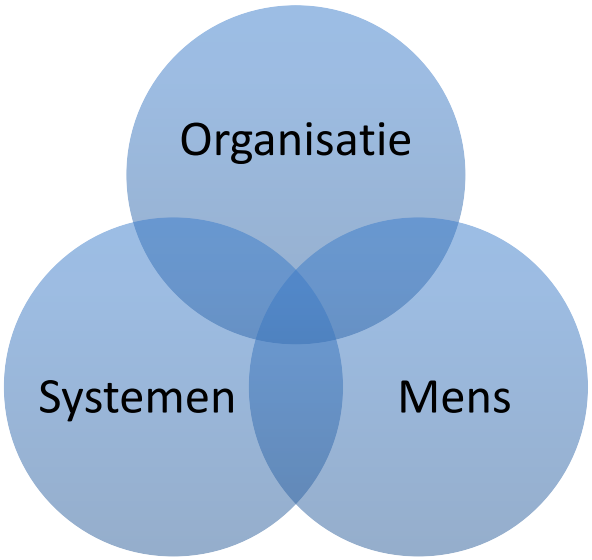
- **Perceptie:**
  De perceptie is het gevoel en beeld/oordeel dat een persoon heeft bij in dit geval het gebruik van zijn gegevens en privacy (7). Deze perceptie komt deels voort uit de informatiekunde maar ook uit de sociologie. Dit begrip kent zowel een positieve als negatieve uitstraling. Dit hangt af van het vertrouwen in de manier waarop gegevens verzameld, verwerkt en doorgegeven worden. De perceptie van de bezoeker zal bepalend zijn bij het wel of niet toestemming verlenen voor de plaatsing van cookies of zichzelf wel of niet herkenbaar maken. De perceptie heeft invloed op de reputatie van de organisatie.

- **Doelgroep/bezoeker:**
  Een groep personen die van belang is in een specifieke situatie. Dit kan gebaseerd zijn op verschillende eigenschappen maar in dit geval gaat het om de websitebezoeker van SNS Bank, en tevens de (potentiële) klant. Hij zal te maken krijgen met de nieuwe gang van zaken en zijn privacy dient beschermt te worden. Daarnaast is zijn perceptie bepalend voor het succes van het marketing systeem en diverse andere activiteiten (waaronder statistieken van de website en het evalueren van tests) van SNS Bank door het wel of niet accepteren van cookies of zichzelf kenbaar te maken.

- **Privacy:**
  Een begrip dat al lange tijd bestaat maar door de opkomende technologieën steeds meer aandacht krijgt. Het hebben van privacy is een recht van de mens (8) (in veel landen opgenomen in de grondwet) en is erg veranderlijk gedurende de jaren (9). Er zijn meerdere soorten privacy. Zo is er privacy in de vorm van persoonlijke vrijheid (het recht om alleen gelaten te worden) en gegevens privacy, wat doelt op welke gegevens van een persoon bewaard en gebruikt mogen worden voor bepaalde doeleinden. Dit laatste is waar het om draait bij technieken die bezoekers kunnen herkennen.

Samenhangend is een geheel van onderdelen te zien zoals in figuur 2.4. Hierin zijn de belangrijkste onderlinge relaties weergegeven, voor allen is wetgeving van toepassing welke zich in de omgeving bevindt. In de omgeving zijn drie hoofdonderdelen waar te nemen, welke ieder uit andere onderdelen bestaan die tevens onderlinge samenhang vertonen (figuur 2.3).

[4] Toezichthouder (tele)communicatie in Nederland.



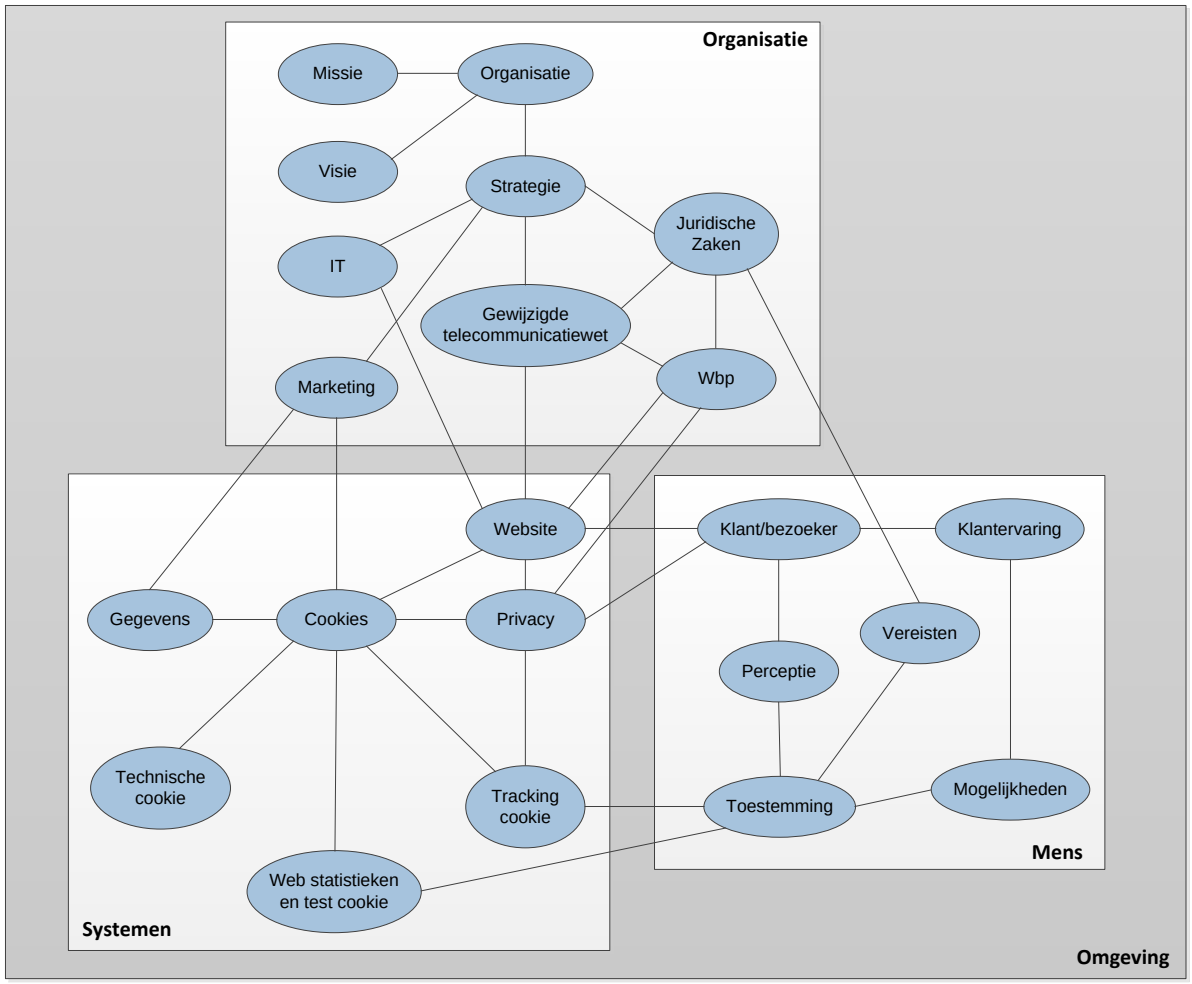
Figuur 2.3 *"Samenhang hoofdonderdelen in omgeving"*

De gehele vraagstelling is een combinatie van de voorgaande punten en begrippen met de nadruk op het van opt-out naar opt-in gaan. De hoofdvraag is dan ook als volgt geformuleerd:

Welke veranderingen dienen er plaats te vinden binnen SNS Bank om te voldoen aan de gewijzigde wetgeving en wat is hierbij de impact op de gebruikerservaring?

Om de hoofdvraag te kunnen beantwoorden zullen achtereenvolgens de volgende deelvragen beantwoord worden:

Deelvraag 1:	Wat zijn cookies en wat zijn de mogelijkheden hiervan?
Deelvraag 2:	Waar worden cookies binnen SNS Bank voor gebruikt?
Deelvraag 3:	Wat zegt de eerdere wetgeving met betrekking tot het gebruik van cookies?
Deelvraag 4:	Wat zegt de gewijzigde wetgeving met betrekking tot het gebruik van cookies en hoe verschilt deze van de eerdere wetgeving?
Deelvraag 5:	Wat zijn de ontwikkelingen bij andere (financiële) organisaties en hoe gaan zij hier mee om?
Deelvraag 6:	Waar dient de oplossing om de interactie tussen bank en bezoeker met cookies te ondersteunen aan te voldoen?
Deelvraag 7:	Welke aanpassingen dienen er gerealiseerd te worden binnen SNS Bank en welke invloed heeft dit?



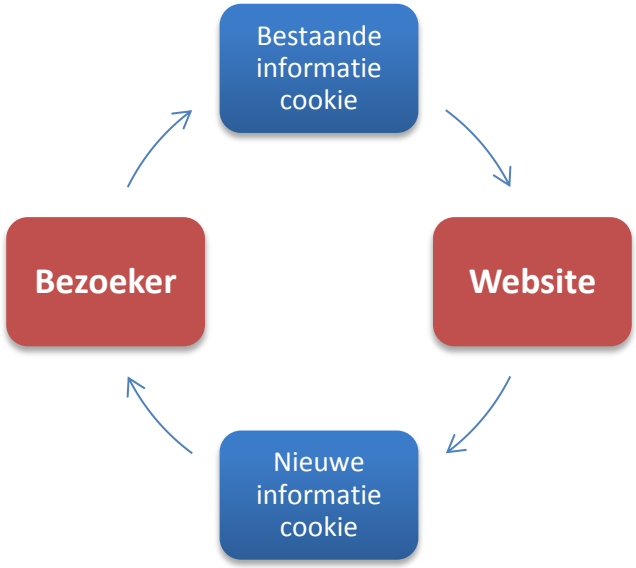
Figuur 2.4 *"De omgeving met verschillende onderdelen en onderlinge samenhang"*

3. EIGENSCHAPPEN VAN COOKIES

Online communicatie kent vele onderdelen en gezien het feit dat de wetgeving sneller haar intrede heeft gedaan dan in eerste instantie werd verwacht komt er meer druk te staan op de beslissing hoe SNS Bank zal gaan handelen. De volgende deelvragen zullen eerst een duidelijk beeld geven van de mogelijkheden van technieken als cookies. Het resultaat hiervan zal vergeleken worden met de huidige situatie bij SNS Bank om vervolgens de nieuwe situatie te kunnen onderzoeken.

3.1 Deelvraag 1: Wat zijn cookies en wat zijn de mogelijkheden hiervan?

Het internet heeft veel mogelijkheden en maakt gebruik van verschillende technieken. Eén daarvan is het plaatsen en uitlezen van informatie op randapparatuur. Hierbij kan een specifieke bezoeker herkend worden. Hiervoor zijn meerdere technieken voorhanden waaronder cookies. Dit zijn kleine tekstbestanden van maximaal vier kilobyte groot die door een website via het internet over het Hypertext Transfer Protocol (HTTP[5]) naar de computer of randapparatuur van een bezoeker gestuurd worden. Wanneer de bezoeker het gebruik van cookies in zijn internetbrowser heeft ingeschakeld (wat de standaardinstelling is) zal de cookie opgeslagen worden en gebruikt worden om gegevens en informatie te bevatten over de bezoeker of klant. De statische manier waarop het internet werkt biedt een eenrichtingstechniek aan, namelijk platte tekst die de internetbrowser omzet in een webpagina. Om ook informatie terug te krijgen, en dus tweerichtingsverkeer te realiseren, worden onder andere cookies gebruikt (figuur 3.1).



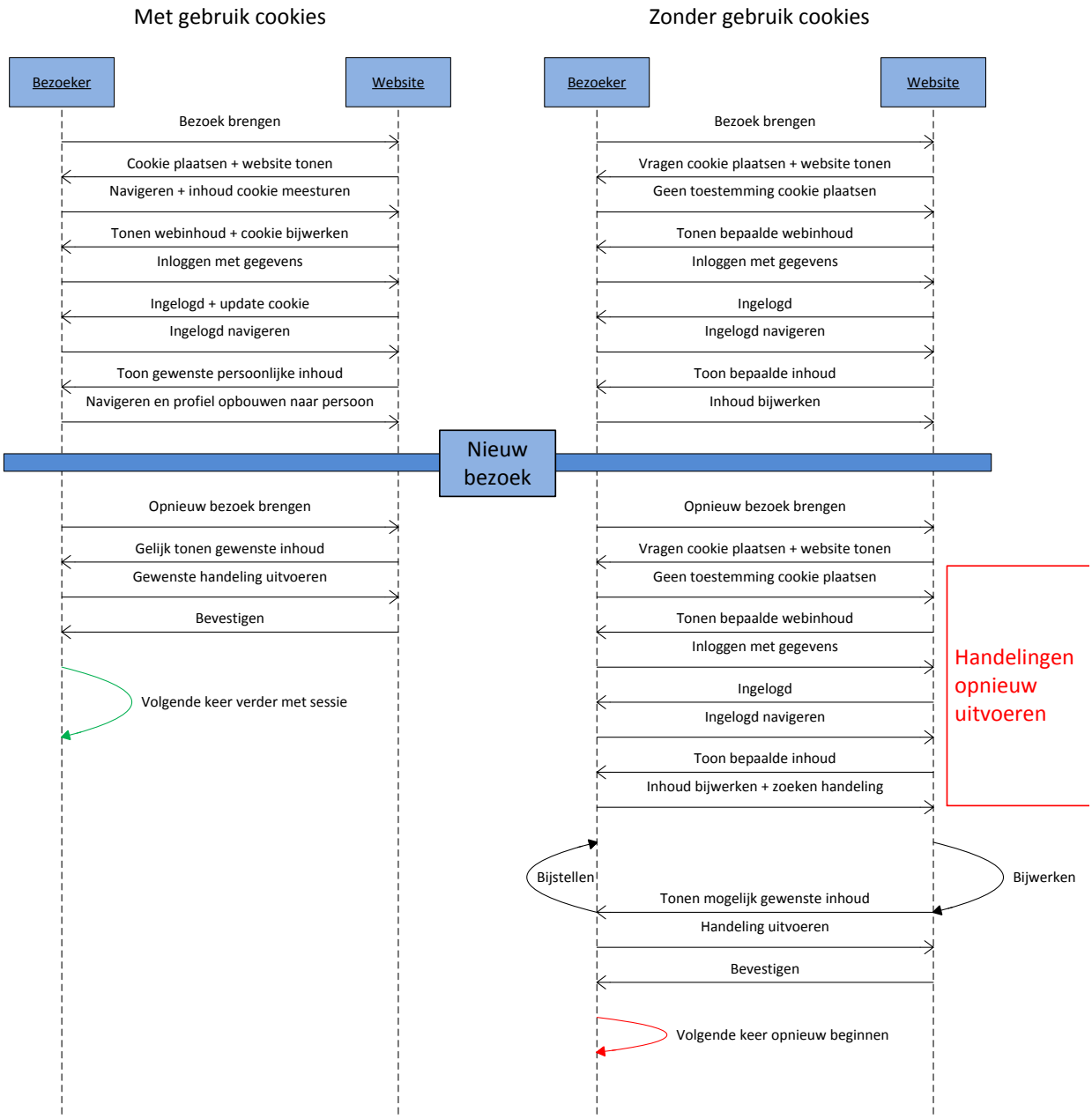
Figuur 3.1 *"Tweerichtingsverkeer met behulp van cookies"*

[5] Voor een website adres staat het protocol, vaak begint dit met http (of https indien de verbinding versleuteld is).

Door het opslaan van gegevens (of een voor de website unieke code) in een cookie en deze aan de website terug te sturen bij een volgend bezoek, of tijdens hetzelfde bezoek, zijn er meer mogelijkheden op het Internet. Voorbeelden zijn het gebruik van web statistieken software, meer gerichte advertenties/zoekresultaten (ook wel behavioural advertising genoemd (10)) maar ook websitevoorkeuren waardoor deze niet bij elk bezoek opnieuw ingesteld moeten worden. Op dit niveau zijn er drie soorten van gebruik te onderscheiden om de bezoeker te herkennen, namelijk:

- Technieken welke gericht zijn op de bezoeker en communicatie tussen website en bezoeker mogelijk maken.
- Technieken welke gericht zijn op de organisatie voor bijvoorbeeld veiligheid en analyse van de website.
- Technieken voor het verzamelen en verwerken van persoonsgegevens. Deze gegevens kunnen zowel met of zonder het informeren van de bezoeker:
    - voor doeleinden binnen de organisatie gebruikt worden.
    - verkocht/doorgegeven worden aan derden.

Bedrijven als Google maar ook webwinkels maken het bezoekers bij gebruik van meerdere categorieën gemakkelijker of in ieder geval doen zij een poging hiertoe. Hierdoor hoeft als het ware niet telkens een nieuwe sessie gestart te worden wat zowel gemak als efficiëntie kan opleveren (figuur 3.2). De ene bezoeker ziet dit als een groot voordeel en de andere niet. Andere bezoekers zijn er niet van op de hoogte en weten niet wat er zich op zijn randapparatuur afspeelt, dit vindt vooral plaats bij de laatste twee categorieën. Het meest extreme geval is om verkregen persoonsgegevens zonder dat de bezoeker hierover geïnformeerd is te verzamelen en aan derden door te geven, dit is echter niet toegestaan. Hierbij kan de privacy van de bezoeker in gevaar komen. Dit is een belangrijke reden waarom de Telecommunicatiewetgeving is gewijzigd.



Figuur 3.2 *"Website bezoeken en handeling uitvoeren met of zonder cookie"*

3.1.1 Technieken

Tegenwoordig zijn er een aantal technieken om een bezoeker op een website te herkennen. Bijvoorbeeld op basis van verborgen velden in HTML formulieren, status aanpassen in de URL of op basis van een IP-adres (11). Dit is echter niet betrouwbaar genoeg en gemakkelijker te manipuleren. Een IP-adres kan bijvoorbeeld meerdere bezoekers hebben (in een netwerk of bij gebruik van een proxy) en is dus niet uniek voor het te gebruiken doel. Een andere optie is het gebruik van 'browser fingerprint'. Deze omstreden techniek leest een (vrijwel) unieke code uit de browser. In combinatie met het gebruik van het IP-adres of andere gegevens zou dit een geschikte vervanger voor cookies kunnen zijn (12). Dit zou dus een serieuze maar meer onopgemerkte manier zijn die schadelijk kan zijn voor privacy. De bezoeker kan hier namelijk geen inzicht in krijgen. De omgekeerde bewijslast is ook hierop van toepassing vanwege het feit dat het terug te herleiden is tot een persoon, het is immers te classificeren als een persoonsgegeven. Daarnaast is er de flash cookie (ook wel 'Supercookie' genoemd). Dit is een cookie die in flash formaat opgeslagen wordt op de randapparatuur van de bezoeker. De inhoud verschilt eigenlijk niet van de normale cookie maar een flash cookie is niet te verwijderen via de gebruikelijke manier. Wanneer de normale cookie door de bezoeker of internet browser verwijderd wordt kan deze als het ware terug gezet worden door de inhoud van de flash cookie, dit verschijnsel is te classificeren als een soort van 'back-up'.

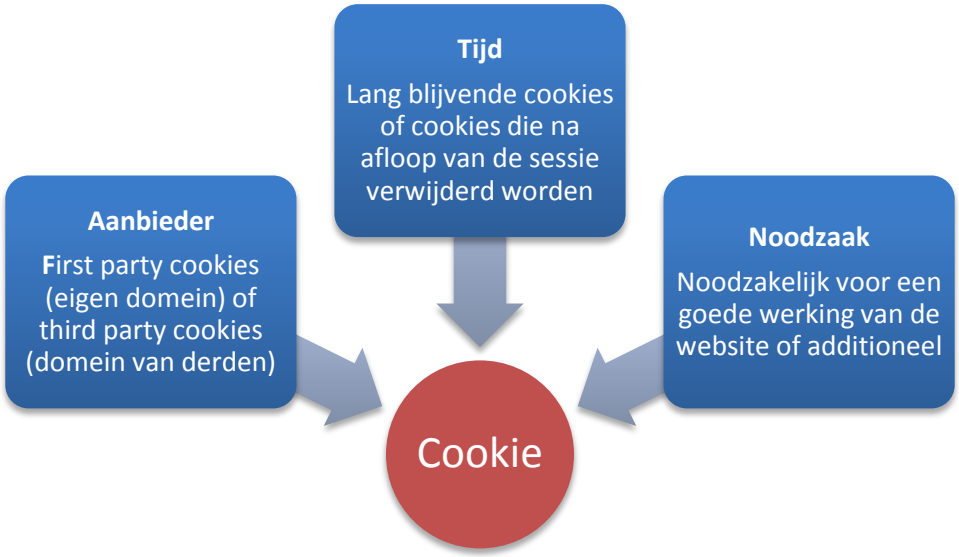
Een techniek die nu op grote schaal ingezet wordt is het gebruik van cookies. Alle technieken voor het herkennen van bezoekers door het plaatsen of uitlezen van gegevens van de randapparatuur zijn door de wetgeving aan banden gelegd. Voor het gebruik hiervan dient daarom toestemming gevraagd te worden. Alternatieve technieken voor het gebruik van cookies, waarop de wet niet van toepassing is en die net zo precies werken, zijn momenteel niet beschikbaar. Het ligt dan ook voor de hand om het al op grote schaal geïmplementeerde gebruik van cookies voort te zetten in plaats van het inzetten van een andere techniek. Eén uitzondering hierop is door de bezoeker te laten inloggen om zo een juridische interactie te bewerkstelligen waarvoor eerder bij registratie een overeenkomst is gesloten. Hierdoor kan de bezoeker er zelf voor kiezen om wel of niet herkend te worden door de website. Deze techniek heeft als voordeel dat deze nog preciezer is dan cookies. Immers is inloggen verbonden aan een persoon en het gebruik van cookies aan specifieke randapparatuur, een apparaat dat ook door meerdere bezoekers gebruikt kan worden. Gezien de marketing doelen die veel gegevens gebruiken is deze manier met de huidige doeleinden niet op grote schaal inzetbaar en daarnaast is het inloggen ondanks de grote controle een extra handeling. Bezoekers zonder inlogmogelijkheid dienen ook herkend te worden voor de verzameling van meer gegevens. Cookies zullen vanwege deze redenen dan ook gebruikt blijven worden.

3.1.2 Eigenschappen van cookies

De inhoud van een cookie kan verschillen. Het kan gaan om de gegevens en instellingen zelf of een unieke code (deze code kan tevens uit de internetbrowser komen, ook wel een 'fingerprint' genoemd). Bij dit laatste houdt de website zelf de instellingen bij maar kan de bezoeker wel herkennen. Hiermee

wordt dus hetzelfde doel bewerkstelligd. Volgens de wetgeving blijkt dat een dergelijke unieke code, ook wel ID, te classificeren is als een persoonsgegeven.

Hierop voortbouwend kan naar (11) gesteld worden dat er een 'impliciet contract' tussen de website en de bezoeker is. De cookie bevat namelijk informatie die voor beide partijen van belang is. De website server rekent erop dat de bezoeker de informatie in de vorm van een cookie bewaart en weer beschikbaar stelt bij een volgend bezoek. De internetbrowser bewaart in principe ook enkel cookies van bezochte websites die de bezoeker zelf bezoekt, deze cookies worden aangeduid als 'First Party cookies'. Uitzondering hierop zijn zogenoemde 'Third party cookies'. De website die bezocht wordt kan deze cookies van derden ook aanbieden. Dit is gelijk één van de soorten cookies die momenteel bestaan en gebruikt worden. Het is namelijk te stellen dat er een onderscheid gemaakt kan worden tussen soorten cookies op basis van drie kenmerkende eigenschappen (figuur 3.3).

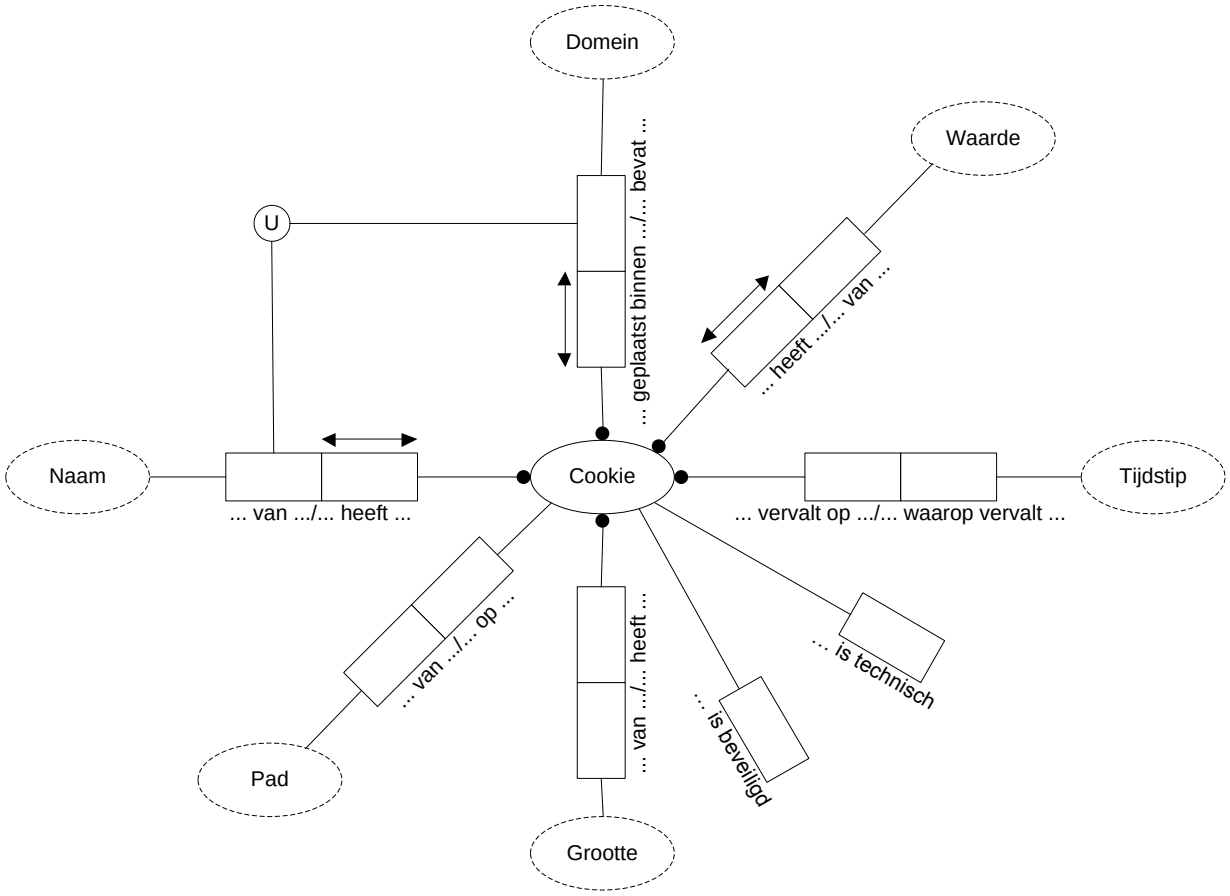


Figuur 3.3 *"Cookies en kenmerkende eigenschappen"*

Aanvullend kunnen bij het plaatsen van een cookie nog enkele andere eigenschappen mee gegeven worden. De aanbieder van de cookie kan aangeven of de cookie binnen een bepaald pad opgeslagen dient te worden of op de standaard locatie van het apparaat (13). Ook is er nog de veiligheidseigenschap welke aangeeft of de cookie over een beveiligde verbinding verzonden dient te worden of juist niet. Momenteel is er ook de eigenschap welke aangeeft via welke TCP poort[6] de cookie verzonden mag worden. Standaard is dit via iedere poort (14).

[6] Transmission control protocol (TCP) ondersteunt het verzenden van gegevens over verschillende poorten om zo meerdere communicatie op hetzelfde systeem mogelijk te kunnen maken. Voor http (webserver) is dit poort 80.

Het ORM[7] model van een cookie en de eigenschappen is weergegeven in figuur 3.4. De eigenschap '… is technisch' duidt aan of een cookie wel of niet technisch is, wat dit inhoudt wordt nog nader toegelicht. Aan de unieke combinatie Domein.Naam kan een cookie herkend worden.



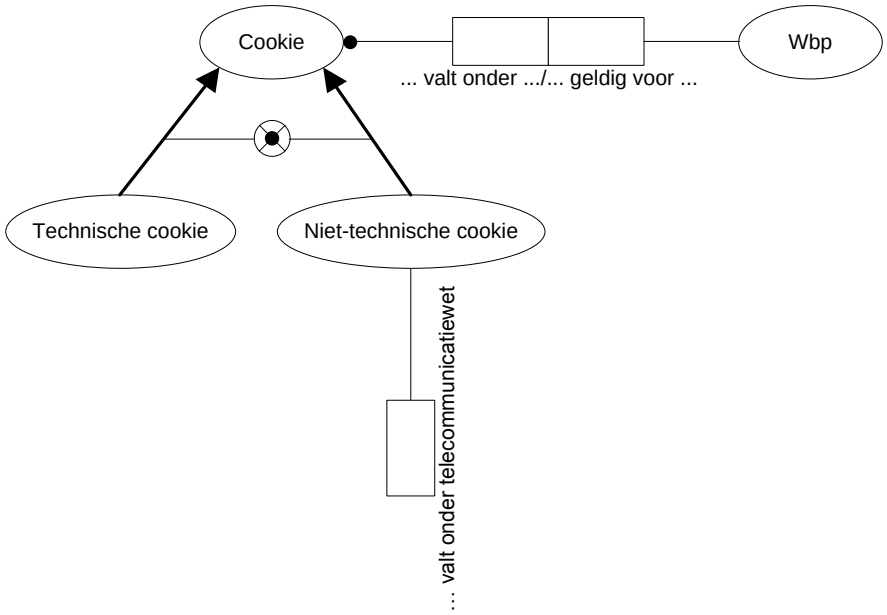
Figuur 3.4 *"Model van een cookie en eigenschappen."*

3.1.3 Technische en niet-technische cookies

De noodzaak voor gebruik van cookies is een belangrijk punt. Technische cookies die noodzakelijk zijn voor een goede werking van de website (communicatie tussen website en bezoeker mogelijk maken) hebben een uitzonderingspositie. Deze cookies zorgen ervoor dat er gecommuniceerd kan worden via het internet of kunnen noodzakelijk zijn om een door de websitebezoeker gevraagde dienst of product te leveren, zo blijkt uit de 'Legal update' binnen SNS REAAL (15). Voorbeelden van dergelijke diensten of producten zijn cookies die het mogelijk maken om in te loggen, inloggegevens onthouden, producten in een winkelmandje te plaatsen en ook voor betalingen.

[7] Object Role Modelling: methode voor het weergeven en controleren van datamodellen.

Niet-technische cookies worden voor andere doeleinden gebruikt. Deze vallen ook onder de Wet Bescherming Persoonsgegevens (Wbp) en kennen dus strengere eisen. Eigenschappen van dit soort cookies zijn het verzamelen, combineren en analyseren van gegevens. Zowel voor commerciële, charitatieve of ideële doeleinden wat dan getypeerd wordt als verwerking van persoonsgegevens en dus valt onder de Wbp (figuur 3.5). In beginsel vallen per 1 januari 2013 alle cookies onder de Wbp. Het deel van de Telecommunicatiewet dat vereist om toestemming te vragen voor het plaatsen van cookies maakt alleen een uitzondering voor technische cookies. Onder niet-technische cookies zijn tracking cookies, web statistieken/analyse cookies en overige/derden cookies te onderscheiden. In figuur 3.5 zijn de geldende onderdelen van de wetgeving aangegeven. Een cookie kan in geen geval als een technische cookie en ook als een niet-technische cookie te classificeren zijn.



Figuur 3.5 *"Soorten cookies en geldende wetgeving"*

Tegenwoordig gebruikt bijna elke website cookies. Dit kunnen zowel First party als Third party cookies zijn en zowel technische als niet-technische cookies. Als bij een bezoek aan een website de bezoeker niet heeft aangegeven geen cookies te willen gebruiken (via een opt-out van de aanbieder of in de instellingen van zijn internetbrowser) zullen vaak meerdere cookies op zijn randapparatuur geplaatst worden. Dit is ook het geval bij de website van SNS Bank. Welke cookies dit zijn is beschreven in de volgende deelvraag.

3.1.4 Privacy

Cookies en andere gelijksoortige technieken kunnen voor onschuldige doeleinden gebruikt worden en de privacy van de bezoeker respecteren. Echter is inbreuk op privacy erg realistisch. Wetgeving is opgesteld om dit tegen te gaan of in ieder geval duidelijke communicatie hierover af te dwingen. Reden

hiervoor is de zelfregulerende 'cookie industrie', waarbij cookies standaard ingeschakeld zijn, door derden geplaatst kunnen worden en informatie gemakkelijk samengevoegd kan worden. Vooral tracking cookies zijn specifiek bedoeld om een bezoeker te volgen in zijn surfgedrag (ook wel klikgedrag) en op basis hiervan een profiel op te bouwen. Gerichte advertenties kunnen dan worden aangeboden op basis van gegevens waarvan de bezoeker niet altijd bewust op de hoogte is dat deze worden verzameld. Wanneer deze gegevens voor een specifiek doel gebruikt worden waar de bezoeker toestemming voor heeft gegeven is dit relatief onschuldig en kan dit door een bezoeker gewaardeerd worden. Dit is echter niet altijd het geval en door middel van dergelijke cookies is in eerste instantie de randapparatuur (bijvoorbeeld een computer) te herkennen maar het is ook mogelijk om de bezoeker te identificeren (16). Naar (4) blijkt dat gegevens privacy onder andere bestaat uit het recht van de bezoeker om zelf te kunnen bepalen welke informatie, en in welke mate, hij prijsgeeft aan een bepaalde partij (in dit geval de aanbieder van de cookie). Dit is bij het gebruik van cookies niet in alle situaties het geval. Na het inloggen en registreren zijn de persoonsgegevens daadwerkelijk bekend. Een geheel andere vorm van cookies is de eerder genoemde 'flash cookie'. Privacy statements met toelichting op het gebruik van cookies noemen deze vorm van cookies vaak ook niet, zo blijkt naar (17). Flash cookies kunnen daarnaast tot honderd kilobyte aan gegevens bevatten in tegenstelling tot de maximale vier kilobyte bij de normale cookie.

Kortgezegd kunnen cookies dus inbreuk maken op de privacy van een persoon. Hierin dienen echter wel nuances aangebracht te worden. Bijvoorbeeld wanneer een aanbieder van cookies deze gegevens strikt gebruikt voor het bekend gemaakte doel en niet verstrekt aan andere partijen. Ook is het een afweging tussen gebruikersgemak en het hebben van privacy. Een website onderhouden kan aanzienlijke kosten met zich mee brengen. Door middel van persoonlijke advertenties gebaseerd op cookies, deze zijn effectiever dan onpersoonlijke advertenties, kunnen deze kosten gedekt worden. De bezoeker dient dan een afweging te maken of hij (gecontroleerd) een deel van zijn privacy in wil leveren voor de te bekijken content of voor meer gebruikersgemak.

Met deze eigenschappen en mogelijkheden van cookies kan nu onderzocht worden in hoeverre de situatie bij SNS Bank hierin is terug te vinden. Zo kan in kaart gebracht worden voor welke specifieke doeleinden cookies gebruikt worden, welke daarvan nodig zijn en welke additioneel.

3.2 Deelvraag 2: Waar worden cookies binnen SNS Bank voor gebruikt?

Binnen het domein van SNS Bank[8] worden net als bij veel andere websites cookies gebruikt. Hierbij betreft het ook verschillende soorten cookies. Het in kaart brengen van de cookies die gebruikt worden is dan noodzakelijk om te bepalen welke cookies daadwerkelijk nuttig zijn en welke niet. Daarnaast is het classificeren aan de hand van de soort nodig om de wijze te bepalen waarop de wetgeving geïmplementeerd dient te worden (bijvoorbeeld als technische of niet-technische cookie). Door de website van SNS Bank te bezoeken wordt duidelijk dat er op de randapparatuur van de bezoeker onmiddellijk enkele cookies geplaatst worden (figuur 3.6). Flash cookies worden er op het gehele domein niet geplaatst.

Bestandsnaam	Aantal
Cookie:gebruikersnaam@snsbank.nl	18
Cookies van derden	5
Totaal:	**23**

Figuur 3.6 *"Cookies bij bezoek startpagina website SNS Bank[9]"*

De opbouw is 'Cookie:' gevolgd door de gebruikersnaam van het account van de bezoeker, een '@' met vervolgens het domein van de aanbieder van de cookie. Op deze wijze kan elke bezoeker herkend worden op hetzelfde apparaat (mits deze een eigen gebruikersaccount gebruikt). De inhoud van de cookies wordt tijdens bezoeken aan andere pagina's continu bijgewerkt. Nieuwe beschikbare informatie wordt toegevoegd of bestaande gegevens worden aangepast. Een deel van de cookies verloopt na de sessie. Dit houdt in dat wanneer de internetbrowser gesloten wordt de cookie zal worden verwijderd. Dit is niet bij alle cookies het geval. Sommigen verlopen gelijk, anderen na een half uur maar een aantal blijft zelfs meerdere maanden of jaren bewaard. Daarnaast is een cookie specifiek voor het betreffende apparaat of de gebruikte browser. Deze kunnen onderling niet uitgewisseld worden. Dit betekent dat een instelling op een tablet niet automatisch ook van toepassing is op een computer. Bij gebruik van een bepaalde browser geldt een opgeslagen cookie specifiek voor die browser en niet ook voor de andere browsers op hetzelfde apparaat.

SNS Bank zelf plaatst bij een bezoek van de bezoeker achttien cookies op de randapparatuur. Dit zijn niet allemaal 'First party cookies' maar ook 'Third party cookies' die via een ander domein geplaatst worden. Dit is een belangrijk verschil. De wetgeving maakt hierin namelijk een essentieel onderscheid. Ook is er nog de situatie dat elke bezochte url[10] andere cookies kan plaatsen. Het bezoeken van de webpagina SNS Bank Sparen (figuur 3.7) levert minder cookies op dan de startpagina (figuur 3.6).

[8] www.snsbank.nl *(Laatst geraadpleegd op 31-12-2012)*
[9] www.snsbank.nl/particulier/home.html *(Laatst geraadpleegd op 31-12-2012)*
[10] Uniform Resource Locator: Webadres dat in de adresbalk wordt ingevoerd en weergegeven.

Bestandsnaam	Aantal
Cookie:gebruikersnaam@snsbank.nl	18
Cookies van derden	1
Totaal:	**19**

Figuur 3.7 *"Cookies bij bezoek webpagina SNS Bank Sparen[11]"*

Er is gekozen voor het onderdeel 'Sparen' gezien het feit dat dit één van de belangrijkste onderdelen van SNS Bank is (2). Hier blijken minder cookies geplaatst te worden dan bij een bezoek aan de startpagina. Dit kan zijn omdat veel bezoekers het pad naar deze pagina bewandelen via de startpagina en de cookies dan al geplaatst zijn of omdat hier minder cookies nodig zijn. Bij het bezoeken van SNS Bank Zakelijk is het resultaat cookies nog minder (figuur 3.8). Daar worden geen cookies door derden geplaatst.

Bestandsnaam	Aantal
Cookie:gebruikersnaam@snsbank.nl	18
Totaal:	**18**

Figuur 3.8 *"Cookies bij bezoek webpagina SNS Bank Zakelijk[12]"*

Per pagina is er dus een verschil qua gebruik van cookies en de verschillende soorten cookies. Voor de implementatie van de gewijzigde wetgeving en het hierop aanpassen van de systemen is het nodig om per cookie te bepalen wat de eigenschappen zijn. Dit gebeurt aan de hand van de aanbieder, tijd en noodzaak (figuur 3.3). Deze data kan vervolgens ingedeeld worden op de manier zoals weergegeven in figuur 3.9. Op basis van de eigenschappen 'First Party cookie', 'Third Party cookie', 'Third Party cookie via eigen' en 'Technische cookie' kan de wetgeving eenduidig opgevat worden.

Domein:	Het internetdomein dat de cookie plaatst.
Aantal:	Het totaal aantal cookies dat geplaatst wordt op een webpagina per domein.
First Party cookie:	Eigen cookie die door het eigen domein, in dit geval snsbank.nl, geplaatst wordt.
Third Party cookie:	Cookie die door een derde partij, bijvoorbeeld Doubleclick, geplaatst wordt.
Third Party cookie via eigen:	Cookie van een derde partij die via het eigen domein geplaatst wordt, bijvoorbeeld van statistiekenprogramma Google Analytics en Omniture via domein snsbank.nl.
Technische cookie:	Cookie die noodzakelijk is om de communicatie met de bezoeker mogelijk te maken of om de bezoeker een product/dienst te kunnen leveren waar hij zelf om heeft gevraagd.

[11] www.snsbank.nl/particulier/sparen.html *(Laatst geraadpleegd op 31-12-2012)*
[12] www.snsbank.nl/zakelijk/home.html *(Laatst geraadpleegd op 31-12-2012)*

Domein	Aantal	First Party cookie	Third Party cookie	Third Party cookie via eigen	Technische cookie
snsbank.nl	18	4	-	14	3
derden	5	-	5	-	-
Totaal:	**23**				

Figuur 3.9 *"Cookies ingedeeld op basis van kenmerkende eigenschappen"*

Gesteld kan worden dat, op deze momentopname voor drie cookies geen toestemming gevraagd moet worden (in dit geval zijn drie van de vier first party cookies ook technische cookies) en voor twintig wel. SNS Bank gebruikt daarnaast van alle soorten cookies minstens één exemplaar. Dit resulteert er uiteindelijk in dat de wetgeving volledig van toepassing is op de gehele website (het domein).

3.2.1 Doeleinden

Momenteel wordt er van de geplaatste cookies veelvuldig gebruikt gemaakt. Het inbound marketing systeem gebruikt cookies om bezoekers te kunnen herkennen en te voorzien van gerichte mededelingen en aanbiedingen. Door cookies kan ingespeeld worden op de behoefte van de bezoekers. Dit is een belangrijke factor in de bedrijfsvoering. Op basis hiervan kunnen bezoekers namelijk bediend worden maar het zorgt ook voor meer (nieuwe) klanten. Op deze wijze is persoonlijke communicatie tussen bezoeker en bank mogelijk. Dit is iets wat bezoekers kunnen waarderen.

Ditzelfde geldt voor de afdeling Internet Verkoop, die op basis van gegevens uit cookies tests uit kan voeren. De cookie dient namelijk als meetinstrument om zo te kunnen leren welke optie van de test het meest effectief, gebruiksvriendelijk of geschikt is. Ook de opgezette (advertentie)campagnes kunnen aan de hand van gegevens, die uit cookies voortvloeien, geëvalueerd worden. Hiermee kan bepaald worden hoe effectief advertenties zijn, hoeveel deze daadwerkelijk opleveren en wat er afgerekend moet worden.

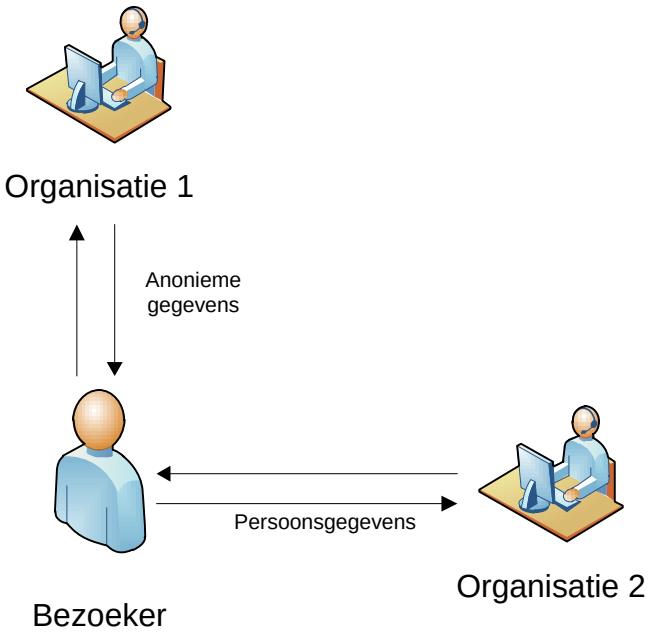
Een ander gebruik van cookies is voor het analyseren van de website, ook wel web statistieken software genoemd. Hiermee kan gemeten worden hoe vaak de website bezocht wordt maar kunnen er ook nog veel meer gegevens verkregen worden om de website te blijven verbeteren aan de behoefte van de bezoeker. Hierdoor kan bijvoorbeeld informatie gemakkelijker gevonden worden. Voortbouwend op analyseren en meten is de situatie bij externe bannering[13]. Hierbij zal gemeten moeten worden wat een banner op een externe website oplevert en hoe effectief deze dus is. De marketing voor campagnes baseert hierop waar wel of niet en op welke wijze een banner geplaatst zal worden. Zonder gegevens over de resultaten is investeren in campagnes en banners op bepaalde websites van derden namelijk niet op doordachte wijze uit te voeren.

[13] Het weergeven van boodschappen (banners/advertenties) op website van derden.

Cookies blijken dus een belangrijk middel te zijn in de bedrijfsvoering van een dergelijke organisatie. Persoonlijke communicatie op transparante wijze maar tegelijkertijd de commerciële factor evalueren en verbeteren zijn van groot belang. In de hele bedrijfsvoering en strategie wordt zo erg geleund op het gebruik van cookies dat deze van groot belang zijn geworden, bij uitschakeling zouden vele systemen niet meer correct of effectief kunnen werken. De omzet kan er daarnaast ook door dalen. In (14) wordt dit ook gesteld: het geheel uitschakelen van cookies of geheel accepteren lijkt niet haalbaar vanwege de vele doeleinden waar cookies voor gebruikt worden, (14) stelt dat hiervoor specifiekere controle nodig is. Het blijkt namelijk, zoals hiervoor beschreven, dat cookies voor vele onschuldige doeleinden gebruikt worden die de privacy niet direct in gevaar brengen. Gezien de verschillende percepties die een bezoeker kan hebben is het beeld van privacy (en eventuele schending hiervan) namelijk erg relatief (7).

3.2.2 Bedreigingen voor privacy

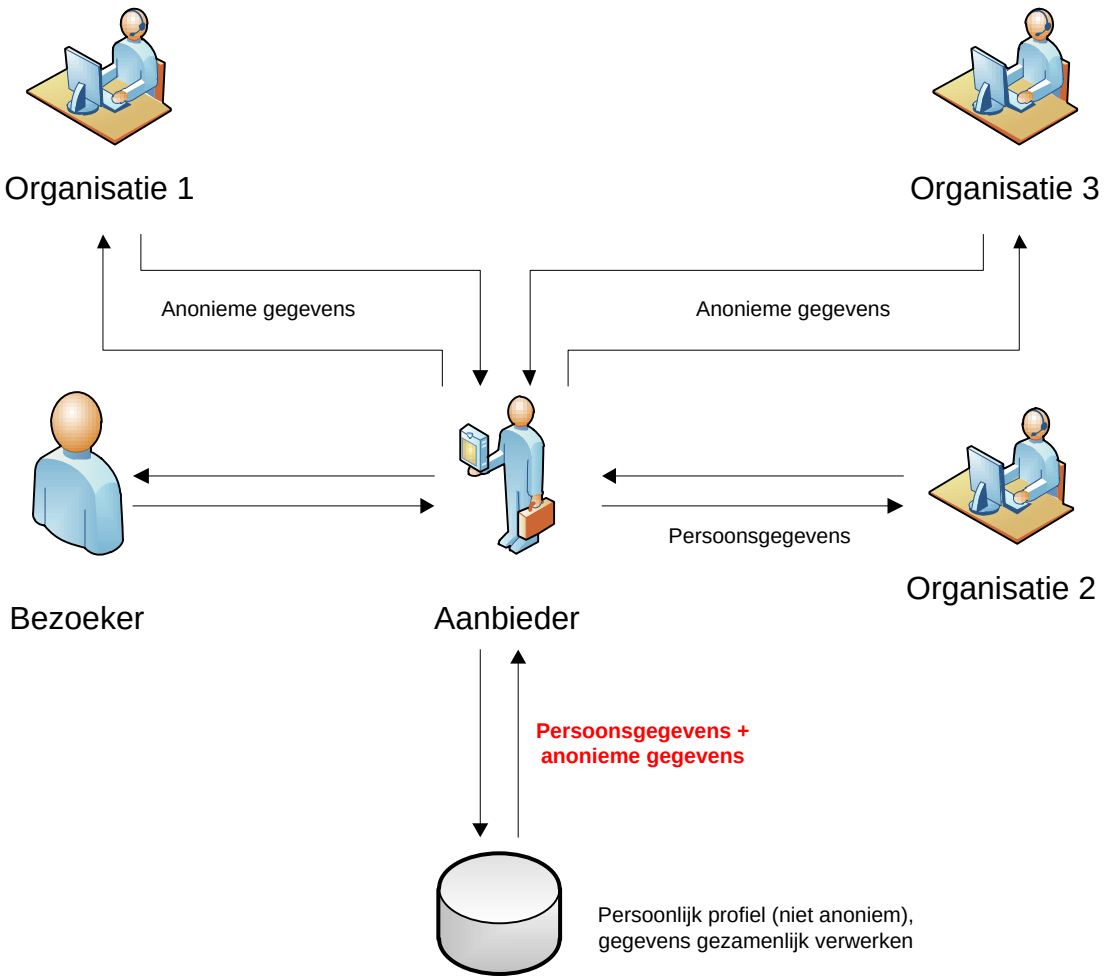
Cookies kunnen voor vele doeleinden ingezet worden, van de meer onschuldige tot bedreigingen voor de privacy. Een belangrijk onderdeel is dat gegevens in bepaalde gevallen wel en in bepaalde gevallen niet zijn te herleiden tot een persoon. Bijvoorbeeld wanneer gegevens als naam, adres en e-mailadres in de cookie zijn opgeslagen of enkel een geanonimiseerd nummer. Eerstgenoemde is in veel gevallen verkregen door bijvoorbeeld registraties op websites of online aankopen. Op deze wijze kunnen gegevens, die voorheen anoniem waren, gekoppeld worden aan een persoon. Op deze wijze kan er een profiel opgesteld worden van een persoon. Dit is ook de voornaamste bedreiging, namelijk het verwerken van de gegevens aan de kant van de organisatie, zo onderschrijft ook (18). Wanneer dit op een specifieke website gebeurt is dit, gezien het feit dat websites technisch alleen hun eigen cookies kunnen uitlezen, niet per direct een bedreiging. De bezoeker is in dat geval op de hoogte wie zijn gegevens verwerkt. Wanneer het een samenwerkingsverband tussen bezoeker en één organisatie is, is de relatie immers helder. Aan ‘Organisatie 1’ wil de bezoeker zich niet kenbaar maken en aan ‘Organisatie 2’ vertrouwt de bezoeker zijn persoonsgegevens wel toe (figuur 3.10).



Figuur 3.10 *"Heldere gegevensverwerking met elke organisatie afzonderlijk"*

Bij derde partijen is het anders, in dat geval zijn de informatiestromen niet geheel helder te onderscheiden. Wanneer een derde partij, zoals een advertentiedienst, advertenties of cookies kan plaatsen op de website van 'Organisatie 1' en 'Organisatie 2' dan kan de advertentiedienst (ofwel aanbieder) over gegevens van beide organisaties beschikken. Dit is een voorbeeld van third party cookies. Wanneer dit bij 'Organisatie 1' en 'Organisatie 3' anonieme gegevens betreffen en bij 'Organisatie 2' persoonsgegevens dan is de advertentiedienst in de gelegenheid om een volledig tot de persoon terug te leiden profiel te genereren op basis van de verschillende cookies (18). Deze situatie is weergegeven in figuur 3.11. De aanbieder van third party cookies zit als het ware tussen de communicatie in. Hierbij kan echter alleen de gespecificeerde communicatie verzameld worden en niet alle communicatie. Ook door 'embedded links' (14), waaronder afbeeldingen, pop-ups, is het mogelijk de gegevens uit cookies van verschillende organisaties (domeinen) te combineren en te verwerken.

Cookies kunnen vooral door onwetendheid van de bezoeker, de subtiele wijze van plaatsing en het gezamenlijk verwerken van informatie schadelijk zijn voor de privacy van de bezoeker. Kwaadwillende organisaties kunnen op deze wijze zeer veel over een persoon te weten kunnen komen, identiteitsdiefstal of creditcardfraude is op deze wijze niet onrealistisch.



Figuur 3.11 *"Geen heldere verwerking van het soort gegevens met organisaties afzonderlijk"*

Op het gebied van wetgeving is er dan ook veel te doen om het gebruik van cookies. Naar (14) blijkt namelijk dat cookies zo fijnmazig zijn verspreid over het gehele internet dat het vermijden van cookies ook erg lastig blijkt te zijn. Hoe dit op het gebied van wetgeving is geregeld wordt in de volgende deelvragen beschreven.

3.2.3 Wijzigingen

Het aantal cookies en bijbehorende eigenschappen zijn aan verandering onderhevig. Dit kan op ieder moment wijzigen, figuur 3.12 onderschrijft dit. Hierin is weergegeven wat de verschillen zijn tussen twee momentopnamen. Op sommige pagina's verdwijnen slechts enkele cookies of komen er enkele bij. Het verschil kan echter ook groter zijn, het grootste verschil is zelfs tien cookies.

Pagina Nr.	Momentopname1	Momentopname2	Verschil
1	23	24	1
2	19	18	-1
3	19	17	-2
4	2	12	10
5	21	21	0
6	21	21	0
7	24	26	2
8	16	16	0
9	18	18	0
10	6	9	3
11	25	24	-1
12	8	8	0
13	24	20	-4
14	21	22	1
15	21	17	-4
16	22	21	-1
17	18	19	1
18	30	28	-2
19	14	11	-3
20	25	20	-5
Totaal	**377**	**372**	**-5**

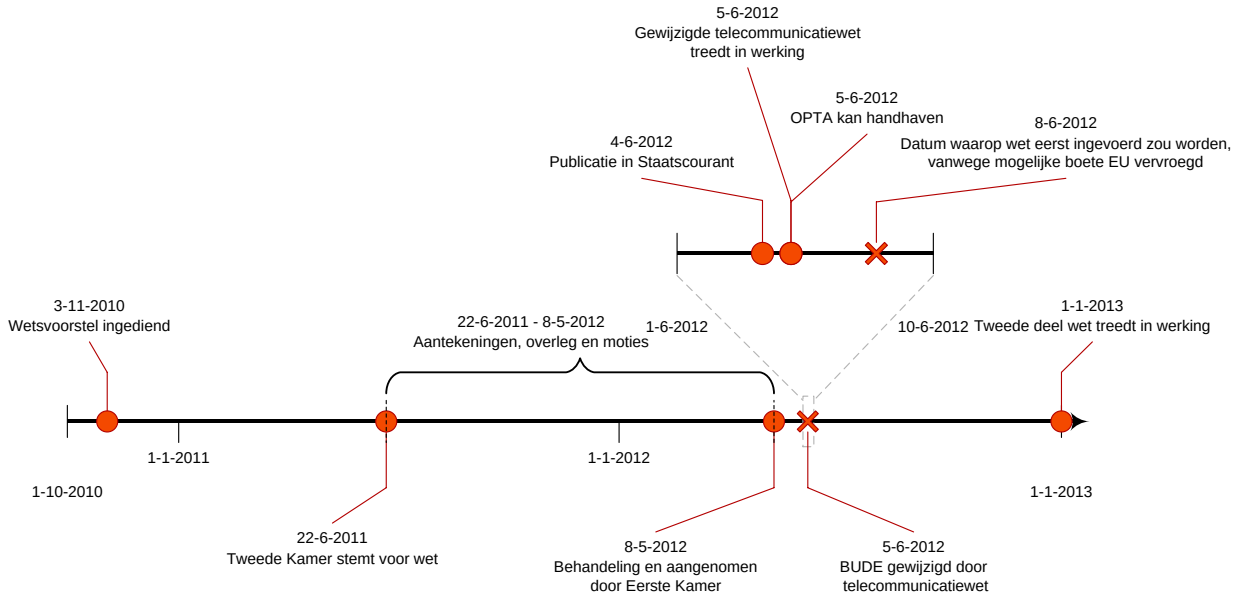
Figuur 3.12 *"Aantallen cookies tussen twee momentopnamen"*

Naast de verschillen in aantallen zijn er ook verschillen in de eigenschappen van de cookies. Soms veranderde het tijdstip waarop deze vervalt. Slechts vijf van de twintig pagina's zijn ongewijzigd gebleven. In appendix 'Details cookies' is te vinden om welke webpagina's het gaat. Het overzicht van cookies dient door deze snel mogelijke wijzigingen een onderhoudbaar proces te zijn.

De mogelijkheden van cookies en waar deze in de situatie van SNS Bank voor gebruikt worden zijn onderzocht. Op basis hiervan kan in het volgende hoofdstuk de toepasbaarheid van de wetgeving bewerkstelligd worden en hierbij zowel de eerdere als de gewijzigde situatie uiteen gezet worden.

4. WETGEVING VOOR GEBRUIK VAN COOKIES

Voorafgaand aan de invoering van de gewijzigde wetgeving, en ook hierna, zijn een aantal momenten te herkennen (figuur 4.1). De eerdere wetgeving wordt uiteengezet en vervolgens zal de nieuwe situatie, met de gewijzigde Telecommunicatiewet beschreven worden.



Figuur 4.1 *"Tijdlijn met betrekking tot de wetgeving"*

4.1 Deelvraag 3: Wat zegt de eerdere wetgeving met betrekking tot het gebruik van cookies?

Al geruime tijd bestaat er wetgeving betreffende telecommunicatie, de bijbehorende technieken en situaties die zich hierbij voor kunnen doen. Wetgeving die ingaat op het gebruik van bestanden of gegevens op randapparatuur is er ook al enkele jaren, deze gaat onder andere in op het gebruik van cookies. Privacybescherming is hiermee ook gereguleerd. De gewijzigde Telecommunicatiewet is dan ook niet geheel nieuw, de wet is enkel gewijzigd. Deze heeft onder meer als doel om de privacy van de burger/bezoeker beter te beschermen. Privacy is namelijk een recht van de mens (8) en daarnaast erg aan verandering onderhevig (9). Vooral door de opkomst van nieuwe media waartoe cookies en bijbehorende technieken ook toe behoren, werd een wetswijziging noodzakelijk geacht. De gewijzigde wetgeving is qua structuur deels anders dan de eerdere wetgeving.

4.1.1 Telecommunicatiewetgeving en Wbp

Gesteld kan ook worden dat er twee wetten van belang zijn, namelijk de Wet bescherming persoonsgegevens (Wbp) en de Telecommunicatiewetgeving. Het betreffende artikel in deze laatstgenoemde wet wordt ook wel aangeduid als 'BUDE', wat staat voor Bescherming Universele Dienstverlening en Eindgebruikersbelangen. Het artikel van deze wet, die in 2004 in deze vorm werd ingevoerd maar door de jaren aangepast is, luidt als volgt:

Artikel 4.1: Bescherming van persoonsgegevens en de persoonlijke levenssfeer

1. Een ieder die door middel van elektronische communicatienetwerken toegang wenst te verkrijgen tot gegevens die zijn opgeslagen in de randapparatuur van een abonnee of gebruiker van openbare elektronische communicatiediensten dan wel gegevens wenst op te slaan in de randapparatuur van de abonnee of gebruiker van openbare elektronische communicatiediensten, dient voorafgaand aan de desbetreffende handeling de abonnee of gebruiker:

a. op een duidelijke en nauwkeurige wijze te informeren omtrent de doeleinden waarvoor men toegang wenst te verkrijgen tot de desbetreffende gegevens dan wel waarvoor men gegevens wenst op te slaan, en

b. op voldoende kenbare wijze gelegenheid te bieden de desbetreffende handeling te weigeren.

2. Het bepaalde in het eerste lid is niet van toepassing, voor zover het de technische opslag of toegang tot gegevens betreft met als uitsluitend doel: de verzending van communicatie over een openbaar elektronisch communicatienetwerk uit te voeren of te vergemakkelijken, of de door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij te leveren en de opslag of toegang tot gegevens daarvoor strikt noodzakelijk is.

De al bestaande wetgeving vereist dat de bezoeker geïnformeerd wordt bij het toegang verkrijgen en/of plaatsen van gegevens op de randapparatuur. Dit betreft onder meer het plaatsen van cookies. Hierbij worden namelijk gegevens op de randapparatuur opgeslagen en later wordt de toegang hiertoe weer verkregen. Wanneer dit het geval is dient de aanbieder van de cookies de bezoeker te informeren dat er cookies gebruikt worden en waarvoor deze gebruikt worden.

Ander belangrijk punt is dat ook duidelijk gecommuniceerd dient te worden hoe cookies geweigerd, en dus ook verwijderd, kunnen worden. Het gaat in dit geval dus om het informeren van de bezoeker en aanbieden van informatie. Hier zijn meerdere manieren voor maar de meest voorkomende is het gebruik van een 'Privacy- en cookiereglement'.

Hierop is ook een uitzondering van kracht. Vertaald naar de situatie van cookies is dit namelijk wanneer het plaatsen van cookies strikt noodzakelijk is. Dit is te vergelijken met de technische cookies.

Daarnaast dient er in Nederland altijd voldaan te worden aan de Wet bescherming Persoonsgegevens (Wbp). Deze wet heeft betrekking op het verzamelen, verwerken en bewaren van persoonsgegevens, dit gebeurt onder andere door het gebruik van cookies. De essentie van de wet in deze context luidt als volgt:

Artikel 8: Wet bescherming persoonsgegevens

a. de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend;

b. de gegevensverwerking noodzakelijk is voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of voor het nemen van precontractuele maatregelen naar aanleiding van een verzoek van de betrokkene en die noodzakelijk zijn voor het sluiten van een overeenkomst;

c. de gegevensverwerking noodzakelijk is om een wettelijke verplichting na te komen waaraan de verantwoordelijke onderworpen is;

d. de gegevensverwerking noodzakelijk is ter vrijwaring van een vitaal belang van de betrokkene;

e. de gegevensverwerking noodzakelijk is voor de goede vervulling van een publiekrechtelijke taak door het desbetreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt, of

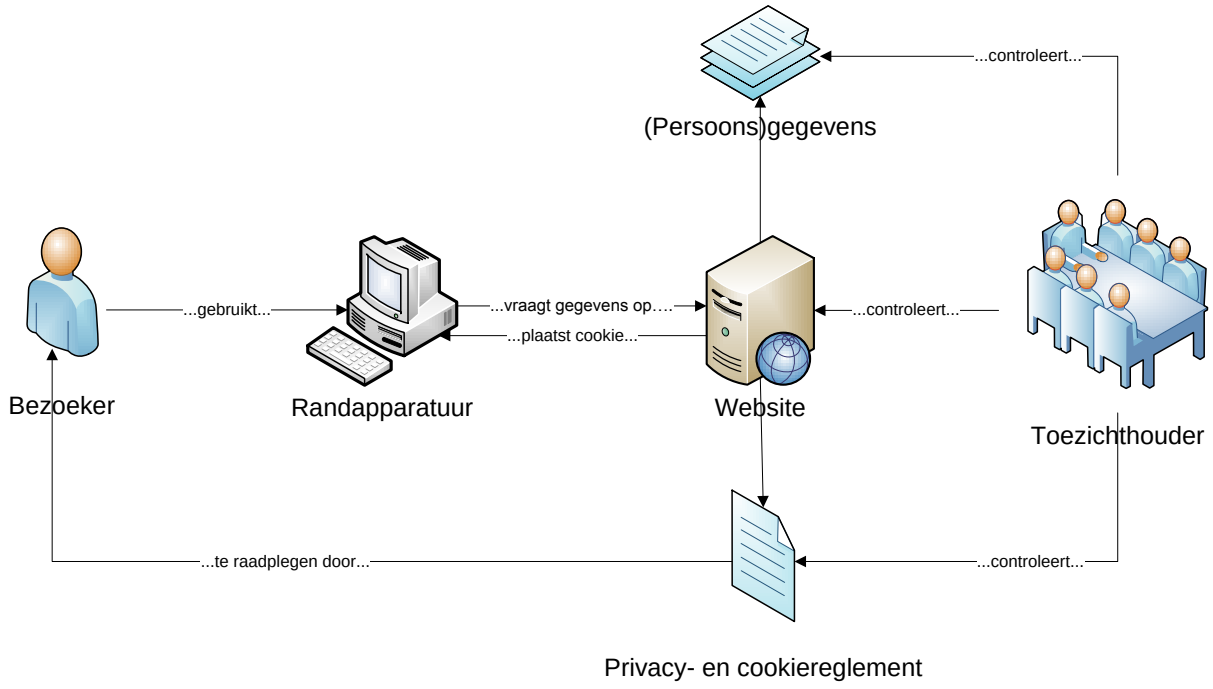
f. de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.

Bij het verwerken van persoonsgegevens moet de reden om dit te doen dus geheel helder zijn. Wanneer hieraan en bijbehorende regels voldaan is dan is verwerking toegestaan. De toezichthouder kan op ieder moment een onderzoek instellen naar de gang van zaken. De bewijslast ligt in dat geval bij de toezichthouder. Wanneer een onjuiste of onwettige verwerking van gegevens geconstateerd wordt dan zal zij dit aan moeten tonen, medewerking van de organisatie is hierbij van belang en ook verplicht.

Concreet kan gesteld worden dat de gehele wetgeving die van toepassing is op de situatie van het gebruik van cookies als volgt te definiëren is:

Bij een bezoek aan een website mogen cookies op de randapparatuur geplaatst worden zo lang de bezoeker tot op zekere hoogte geïnformeerd wordt dat dit gebeurt, waarom dit gebeurt en hij inzicht kan hebben in zijn persoonsgegevens die verwerkt worden. De toezichthouder kan de gang van zaken onderzoeken en bij onjuistheden met de juiste bewijsvoering ingrijpen.

In figuur 4.2 is de omgeving te zien waarin dit speelt. Op dit gedeelte heeft de wetgeving momenteel betrekking.



Figuur 4.2 *"Gang van zaken bij gebruik van gegevens"*

De 'Gedragscode Verwerking persoonsgegevens Financiële instellingen', opgesteld door de Nederlandse Vereniging van Banken (NVB) en het verbond van verzekeraars, gaat hier verder op in. Deze gedragscode onderstreept het voorgaande:

"Een Financiële instelling die elektronische contactgegevens voor elektronische berichten (zoals e-mail, sms-berichten, mms-berichten) heeft verkregen in het kader van de verkoop van een financieel product of het verlenen van een financiële dienst mag deze gegevens gebruiken voor Direct Marketing ten behoeve van eigen gelijksoortige financiële producten of financiële diensten ("soft opt-in"). In dat geval moet de Betrokkene wel steeds gewezen worden op zijn absolute recht van verzet om dit gebruik terstond te laten beëindigen ("opt-out")." (19)

4.1.2 Privacy- en cookiereglement

Noodzakelijk onderdeel binnen het onder de aandacht brengen van privacy en bescherming hiervan, is het privacy- en cookiereglement. Hoofdtaak is om duidelijkheid te verschaffen over wat er met persoonsgegevens gebeurt en is opgesteld voor de bezoeker vanuit juridisch oogpunt. In dit document staan artikelen die volgens wetgeving verplicht zijn gesteld om aan te voeren bij het aanbieden van online diensten. Hieronder valt ook informatie over het plaatsen van cookies. Aan de hand van het privacy- en cookiereglement van SNS Bank kan dit toegelicht worden. In deze specifieke situatie is de Wbp nader uitgewerkt tot de 'Gedragscode Verwerking persoonsgegevens Financiële instellingen' (19). De algemene hoofdlijnen van het privacy- en cookiereglement van SNS Bank zijn:

- Privacybeleid
- Doeleinden waarvoor gegevens verwerkt worden
    - Verwerking bijzondere gegevens (onder andere voor de overheid)
    - Opnemen contact
- Gebruik van de website
    - Cookies van SNS Bank
    - Personaliseren van de website
    - Mededelingen op maat binnen Mijn SNS
    - Overig gebruik klantprofiel
    - Cookies van derden
    - Blokkeren van cookies
    - Hyperlinks
- Inzage, correctie en wijziging persoonlijke gegevens

De in het kader weergegeven onderdelen zijn in dit geval van belang. De bezoeker wordt door middel van het privacy statement geïnformeerd dat er cookies gebruikt worden, waarvoor deze gebruikt worden en welke gegevens er verwerkt worden. Hiermee wordt voldaan aan de eisen van de wet. Ook de mogelijkheid om cookies te kunnen blokkeren wordt toegelicht.

Met de gewijzigde wetgeving zijn enkele verschillen te herkennen ten opzichte van de eerdere situatie. De volgende deelvraag gaat hier uitvoerig op in. Hierop gebaseerd is te bepalen welke veranderingen doorgevoerd dienen te worden om te voldoen aan de gewijzigde wetgeving.

4.2 Deelvraag 4: Wat zegt de gewijzigde wetgeving met betrekking tot het gebruik van cookies en hoe verschilt deze van de eerdere wetgeving?

De gewijzigde wetgeving brengt een aantal ingrijpende veranderingen met zich mee voor alle websites in Nederland. Zoals weergegeven in figuur 4.1 is de wet onder te verdelen in twee delen, te weten het gedeelte dat ingaat op cookies en de Wbp. Voorheen was het plaatsen van alle cookies zonder toestemming toegestaan, nu zal daar toestemming voor gevraagd moeten worden. De Nederlandse overheid stelt kort het volgende op haar website:

"Ook de zogenaamde cookiebepaling treedt op 5 juni in werking: internetgebruikers moeten beter worden geïnformeerd over cookies. Ze mogen niet zonder toestemming van de internetgebruiker op zijn computer worden geplaatst. Toezichthouders, in het bijzonder de OPTA, krijgen met de wetswijziging meer instrumenten voor een effectief markttoezicht."[14]

De gewijzigde Telecommunicatiewet kent een artikel dat specifiek in gaat op het plaatsen en uitlezen van gegevens op randapparatuur van de bezoeker, dit betreft artikel 11:

[14] www.rijksoverheid.nl/onderwerpen/ict/nieuws/2012/06/04/gewijzigde-telecommunicatiewet-in-werking-op-5-juni.html *(Laatst geraadpleegd op 31-12-2012)*

Artikel 11.7a: Telecommunicatiewet

1. Onverminderd de Wet bescherming persoonsgegevens dient een ieder die door middel van elektronische communicatienetwerken toegang wenst te verkrijgen tot gegevens die zijn opgeslagen in de randapparatuur van een gebruiker dan wel gegevens wenst op te slaan in de randapparatuur van de gebruiker:

a. de gebruiker duidelijke en volledige informatie te verstrekken overeenkomstig de Wet bescherming persoonsgegevens, en in ieder geval omtrent de doeleinden waarvoor men toegang wenst te verkrijgen tot de desbetreffende gegevens dan wel waarvoor men gegevens wenst op te slaan, en

b. van de gebruiker toestemming te hebben verkregen voor de desbetreffende handeling.

Een handeling als bedoeld in de aanhef, die tot doel heeft gegevens over het gebruik van verschillende diensten van de informatiemaatschappij door de gebruiker of de abonnee te verzamelen, combineren of analyseren voor commerciële, charitatieve of ideële doeleinden, wordt vermoed een verwerking van persoonsgegevens te zijn, als bedoeld in artikel 1, onderdeel b, van de Wet bescherming persoonsgegevens.

2. De in het eerste lid, onder a en b, genoemde vereisten zijn ook van toepassing in het geval op een andere wijze dan door middel van een elektronisch communicatienetwerk wordt bewerkstelligd dat via een elektronisch communicatienetwerk gegevens worden opgeslagen of toegang wordt verleend tot op het randapparaat opgeslagen gegevens.

3. Het bepaalde in het eerste en tweede lid is niet van toepassing, voor zover het de technische opslag of toegang tot gegevens betreft met als uitsluitend doel:

a. de communicatie over een elektronisch communicatienetwerk uit te voeren, of

b. de door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij te leveren en de opslag of toegang tot gegevens daarvoor strikt noodzakelijk is.

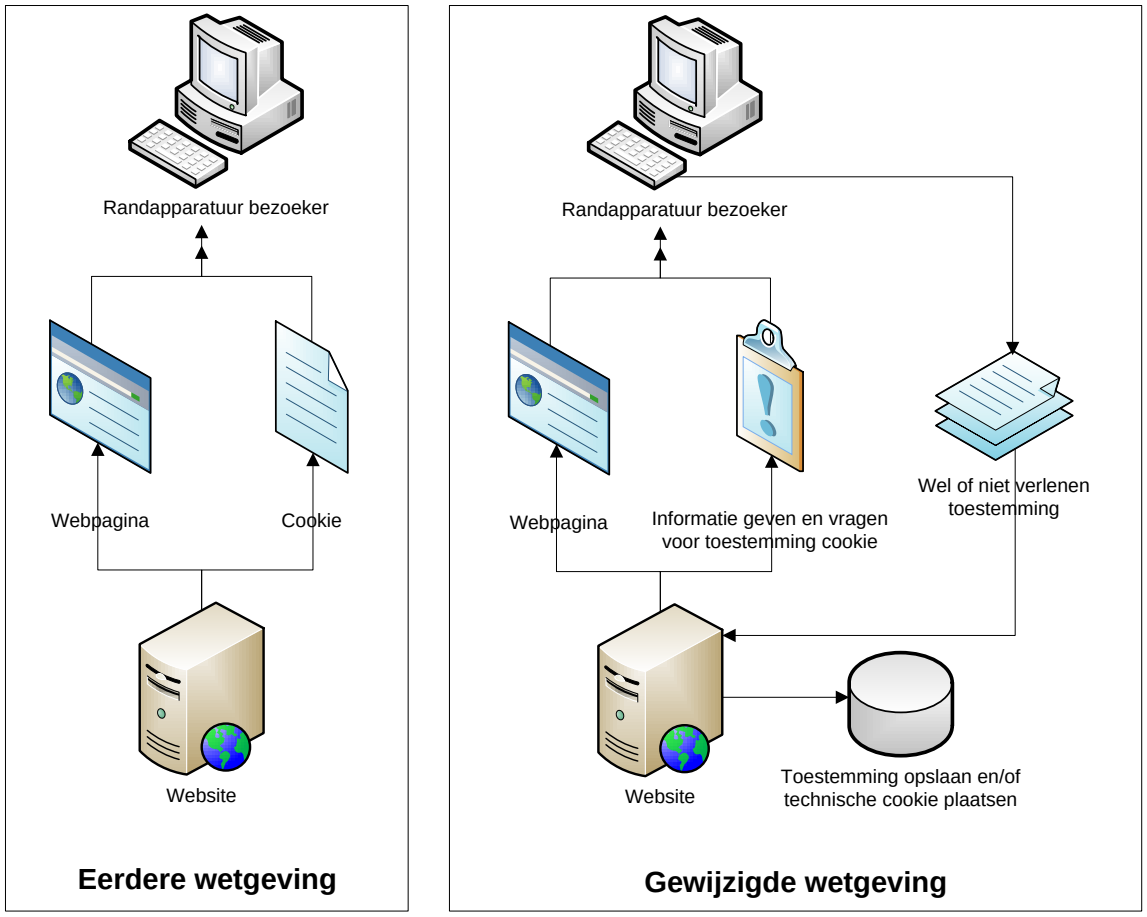
4. Bij algemene maatregel van bestuur kunnen in overeenstemming met Onze Minister van Veiligheid en Justitie nadere regels worden gegeven met betrekking tot de in het eerste lid, onder a en b, genoemde vereisten. Het College bescherming persoonsgegevens wordt om advies gevraagd over een ontwerp van bedoelde algemene maatregel van bestuur.

Dit is in meerdere opzichten anders dan de eerdere wetgeving. Het is te stellen dat deze gewijzigde wetgeving nu kort gezegd het volgende vereist:

- Hoofdregel:
  - De bezoeker informeren over het gebruik van (niet-technische) cookies
  - Expliciet toestemming vragen voor het plaatsen van (verschillende soorten) cookies alvorens deze daadwerkelijk te plaatsen.

- Uitzonderingen hierop:
  - Er is geen toestemming nodig voor cookies die noodzakelijk zijn om de communicatie met de bezoeker mogelijk te maken.
  - Er is geen toestemming nodig als een cookie noodzakelijk is om de bezoeker een product/dienst te kunnen leveren waar hij zelf om heeft gevraagd.

Het meest cruciale verschil ten opzichte van de eerdere wetgeving is dus het informeren en daarnaast het toestemming vragen. In figuur 4.3 is de gang van zaken bij zowel de eerdere als de gewijzigde wetgeving uiteengezet.



Figuur 4.3 *"Situatie eerdere en gewijzigde wetgeving"*

Toen de eerdere wetgeving van kracht was kon een cookie gelijk geplaatst worden op de randapparatuur van de bezoeker bij het bezoeken van een webpagina. Bij de gewijzigde wetgeving ligt dit een stuk complexer. Er dient bij het bezoeken van de webpagina eerst gevraagd te worden om toestemming van de bezoeker alvorens de cookie te plaatsen op de randapparatuur. De bezoeker kan deze toestemming, op basis van de verplicht te verstrekken informatie over cookies, wel of niet geven. Deze toestemming dient vervolgens opgeslagen te worden in een bestand en/of in een technische cookie die alsnog geplaatst wordt op de randapparatuur van de bezoeker. Dit is toegestaan, het betreft een uitzondering op de gewijzigde wetgeving (zie ook figuur 3.5).

4.2.1 Voorbeelden

Eén van de eerdere uitgewerkte en werkende voorbeelden is de website van het Information Commissioner Office (ICO)[15], deze organisatie is toezichthouder in Groot Brittannië (te vergelijken met de OPTA in Nederland). Op de website van deze organisatie wordt daadwerkelijk om toestemming gevraagd. Dit gebeurt door middel van een balk bovenaan de website met daarin de tekst “The ICO would like to place cookies on your computer to help us make this website better. To find out more about the cookies, see our privacy notice.” Daarbij is ook een checkbox (vakje waarin de bezoeker een vinkje dient te zetten indien hij akkoord gaat) te vinden met daarbij de tekst “I accept cookies from this site.” Door het vakje aan te vinken en vervolgens op ‘Continue’ te drukken geeft de bezoeker expliciet toestemming om cookies op zijn randapparatuur te laten plaatsen. De ‘privacy notice’ is gemakkelijk te bereiken en geeft inzicht in het gebruik van cookies. Er is vermeld waarvoor cookies gebruikt worden maar daarnaast ook in tabelvorm de naam en het specifieke doel van de cookie. Ook is per cookie meer informatie te bereiken.

De website voldoet in dit opzicht aan de wetgeving die in Nederlands geldig is (ondanks dat het een website uit Groot Brittannië betreft) omdat de bezoeker geïnformeerd wordt en er expliciet toestemming gevraagd wordt voor het plaatsen van cookies. Dit blijkt ook bij analyse van de website. Er worden geen cookies geplaatst bij een bezoek totdat het vinkje is geplaatst en de bezoeker dus toestemming heeft verleend. Bij het accepteren van cookies is het resultaat zoals weergegeven in figuur 4.3.

[15] www.ico.gov.uk *(Laatst geraadpleegd op 31-12-2012)*

Domein	Vervalt	Naam	First Party	Third Party	Third Party via eigen
.ico.gov.uk	Sat, 16 Aug 2014 13:44:41 GMT	__utma			X
.ico.gov.uk	Thu, 16 Aug 2012 14:14:41 GMT	__utmb			X
.ico.gov.uk	Fri, 01 Jun 2012 11:09:08 GMT	__utmc			X
.ico.gov.uk	sessie	__utmz			X
.ico.gov.uk	Fri, 15 Feb 2013 01:44:41 GMT	ICOCookiesAccepted	X		
	: Technische cookie (functioneel)				

Figuur 4.3 *"Cookies en eigenschappen bij bezoek startpagina ICO"*

Door het toestaan van cookies wordt web statistieken software geactiveerd en hiervoor worden vier cookies gebruikt. Daarnaast is er één technische cookie te vinden, deze registreert of de bezoeker toestemming heeft gegeven voor het plaatsen van cookies op zijn randapparatuur (true of false). Of het tweede gedeelte van de wet (Wbp, omgekeerde bewijslast) ook stand houdt is de vraag. Immers blijkt naar (11) dat de website de bezoeker vertrouwt in het bewaren van deze cookie. Wanneer de bezoeker deze verwijderd is het lastig voor de website aan te tonen dat de bezoeker expliciet toestemming heeft verleend, tenzij er een ander log bestand (in beheer van de website) bestaat waarin dit nauwkeurig opgeslagen wordt.

Een Nederlands voorbeeld is de website van de publieke omroep[16]. Bij bezoek verschijnt een pop-up met de vraag om toestemming en hierin wordt informatie gegeven over het doel waarvoor de cookies gebruikt worden. De technische cookies worden logischerwijs wel geplaatst maar voor de web statistieken cookies (analyse cookies die anonieme gegevens verzamelen) is toestemming van de bezoeker nodig. Wanneer de bezoeker geen toestemming geeft kan hij de website niet bezoeken. De publieke omroep kan deze statistieken dan namelijk niet verzamelen, iets wat vanuit de wetgeving wel verplicht is gesteld. Hierbij wordt duidelijk dat de gewijzigde wetgeving meer impact heeft dan waarvoor deze bedoeld is.

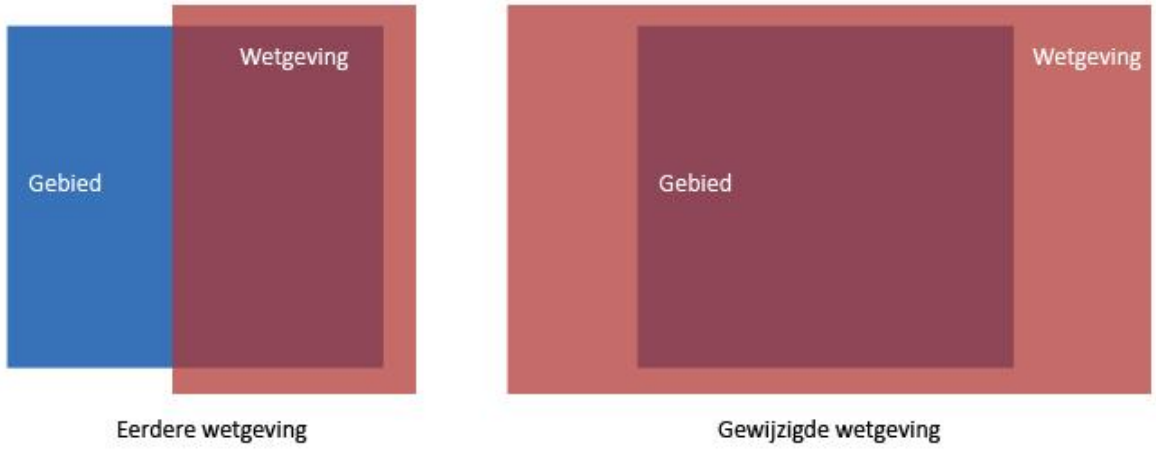
De komende tijd zullen er steeds meer websites om toestemming voor het plaatsen van cookies vragen. Zo ook de website van de Radboud Universiteit Nijmegen[17]. De manier waarop kan verschillen, net zoals voor welke cookies en in hoeverre de toestemming expliciet gegeven is. Ook het niveau en de detaillering van informatie is erg wisselend.

4.2.2 Bereik van de wetgeving

Op basis van het voorgaande is te stellen dat de wetswijziging, die de bezoeker in zijn privacy wil beschermen, verregaande gevolgen heeft. Zowel voor de organisatie als voor de bezoeker. Figuur 4.4 geeft de situatie weer met betrekking tot de wetgeving. De gewijzigde wetgeving is wellicht te drastisch

[16] www.publiekeomroep.nl *(Laatst geraadpleegd op 31-12-2012)*
[17] www.ru.nl *(Laatst geraadpleegd op 31-12-2012)*

voor het bestaande (probleem)gebied. In de huidige situatie kan het een te brede/veelomvattende wetgeving zijn. Een nuance hierin zou op zijn plaats kunnen zijn.



Figuur 4.4 *"Bereik van de wetgeving"*

Vooralsnog is deze nuance niet aanwezig en aangezien wetgeving nageleefd dient te worden zal er voor alle niet-technische cookies toestemming gevraagd dienen te worden. Desondanks zal een nuance in de toekomst niet onrealistisch zijn. Vooral op het gebied van analyse cookies die enkel anonieme gegevens verzamelen.

4.2.3 Omgekeerde bewijslast

Het tweede deel van de gewijzigde wetgeving betreft de omgekeerde bewijslast, dit is anders dan bij de eerdere wetgeving. Bij het verwerken van persoonsgegevens moet de reden om dit te doen altijd volstrekt helder zijn. Wanneer hieraan en bijbehorende regels voldaan is dan is verwerking toegestaan. De toezichthouder kan net als bij de eerdere wetgeving op ieder moment onderzoek instellen naar de gang van zaken. De bewijslast ligt bij de gewijzigde wetgeving echter bij de organisatie. De organisatie zal aan de toezichthouder moeten aantonen dat bij gebruik van cookies alles volgens de geldende wetgeving gebeurt en of er wel of niet persoonsgegevens verwerkt worden en het zodoende wel of niet onder de Wbp valt.

"Als een cookie wordt geplaatst:

- *om gegevens te verzamelen, combineren of te analyseren;*
- *voor commerciële, charitatieve of ideële doeleinden;*
- *dan wordt dit vermoedt een verwerking van persoonsgegevens te zijn in de zin van de Wbp.*

Deze cookies worden aangeduid als tracking cookies. Voor tracking cookies moet dus niet alleen toestemming worden gevraagd om deze te plaatsen, het gebruik van deze cookies moet daarnaast voldoen aan alle regels uit de Wbp." (15)

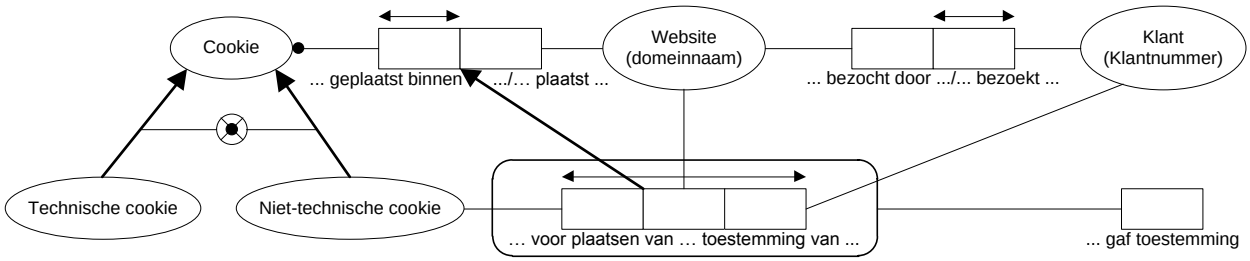
Concluderend kan gesteld worden dat zowel de expliciete toestemming als de manier waarop gegevens (en welke gegevens) verwerkt worden moet voldoen aan de Wbp en daarnaast overeen dient te komen met de beschrijving in het privacy- en cookie statement.

Aanvullend, maar niet nieuw, is het bewaren van deze gegevens, conform de wetgeving en deze beschikbaar te houden (voor opsporingsinstanties en de toezichthouder). In de nieuwe situatie, waarin aangetoond moet worden dat een bezoeker expliciet toestemming heeft gegeven voor het plaatsen van cookies, zal dit vastgelegd moeten worden. Toezichthouder OPTA kan dit opeisen om de gang van zaken te controleren. Er zullen dus gegevens vastgelegd moeten worden, die de toestemming aantonen in voor de OPTA aanvaardbare mate en de privacy van de bezoeker respecteren. Volgens de 'Algemene wet bestuursrecht' artikel 5.45 vervalt de mogelijkheid om een bestuurlijke boete op te leggen vijf jaar nadat de overtreding heeft plaatsgevonden. De hoogte van het boetebedrag is bepalend voor deze termijn. Wanneer de mogelijk op te leggen bestuurlijke boete meer dan € 340 kan bedragen, wat het geval is bij de gewijzigde Telecommunicatiewetgeving (tot een maximum van € 450.000), is dit vijf jaar, zo blijkt uit verwant artikel 5.53. De organisatie zal dus vijf jaar lang moeten kunnen aantonen dat een specifieke bezoeker daadwerkelijk expliciet toestemming heeft gegeven voor het plaatsen van cookies. Dit vergt dus een aanpassing in de achterliggende systemen, welke op hun beurt ook de privacy en bescherming hiervan dienen te waarborgen. Dit dient bewaart te worden, ook wanneer de cookie achteraf verwijderd is. Een log bestand, zoals een database, om de verwerking van toestemming vast te leggen, ligt daarom het meest voor de hand ondanks de extra benodigde capaciteit die dit met zich mee brengt.

Het is duidelijk dat er door de wetgeving (het eerste deel hiervan) een aantal wijzigingen dient plaats te vinden op het gebied van techniek en de bedrijfsvoering. Het volgende hoofdstuk zet de mogelijke opties met bijbehorende afwegingen uiteen. Online communicatie zal veranderen en daarmee ook de situatie voor SNS Bank. Waar de mogelijk oplossing in ieder geval aan dient te voldoen is vastgesteld met behulp van de requirements. In het volgende hoofdstuk wordt hier nader op ingegaan.

5. HET COOKIE VRAAGSTUK

Op basis van de voorgaande hoofdstukken kan het geheel weergegeven worden zoals in figuur 5.1. De gang van zaken voor toestemming vragen is hier schematisch te zien.



***Figuur 5.1** "Het 'Cookie vraagstuk'"*

Altijd wanneer er een 'Niet-technische' cookie geplaatst is voor een bepaalde bezoeker op een website dient hier een toestemming voor gegeven te zijn. Ofwel, zonder toestemming dienen er geen 'niet-technische' cookies gebruikt te worden. Samengevat in een model is dit het 'Cookie vraagstuk'. Met de informatie uit voorgaande hoofdstukken wordt nu naar de datgene toegewerkt waar een mogelijke oplossing aan dient te voldoen.

5.1 Deelvraag 5: Wat zijn de ontwikkelingen bij andere (financiële) organisaties en hoe gaan zij hier mee om?

De gewijzigde wetgeving is daadwerkelijk nieuw in de zin dat organisaties niet weten hoe zij hieraan kunnen voldoen. De manier is dermate vernieuwd en anders dat er geen 'perfecte manier' voorhanden is. Dit zorgt ervoor dat organisaties zelf aan de wet moeten voldoen op een zelf te bepalen manier. Ook toezichtophouder OPTA geeft geen concrete manier voor implementatie op de website. Er is dus onderzoek nodig om te bepalen wat de te kiezen strategie gaat worden. De implementatie op de website van de organisatie zal ook nader uitgewerkt moeten worden. Het is te stellen dat er in ieder geval enkele onderdelen te onderscheiden zijn waaraan voldaan dient te worden, te weten:

1. Informeren
2. Toestemming vragen
3. Toestemming verwerken in website
4. Toestemming opslaan
5. Verwerking (persoons)gegevens controleren/aantonen

***Figuur 5.2** "Onderdelen waaraan voldaan dient te worden"*

Nederlandse organisaties zijn zoekende hoe dit gerealiseerd kan worden. Zowel op juridisch gebied, als op marketing en IT technisch gebied. Er verschijnen na de invoering van de gewijzigde wetgeving verschillende opvattingen en implementaties op websites. Dat er nog veel onduidelijkheid heerst, blijkt uit het feit dat twee maanden na de invoering van de wetgeving slechts een klein aantal websites informeert, laat staan toestemming vraagt en verwerkt. In een onderzoek (20) dat de OPTA ongeveer gelijktijdig publiceerde blijkt dat van de top vijfentwintig Nederlandse website, zes websites de bezoeker actief informeren dat zij cookies plaatsen en gebruiken en dit ook op een opvallende manier doen. Eén website vraagt ook daadwerkelijk toestemming alvorens het plaatsen van cookies. Daarnaast is niet eenduidig welke cookies wel technisch zijn (en waar dus geen toestemming voor gevraagd hoeft te worden) en welke niet. Ook bij de Nederlandse overheid is de wet niet geheel duidelijk, zo blijkt uit berichten uit de media. Zij stelde namelijk dat haar website[18] niet aan de wetgeving hoeft te voldoen aangezien de cookies niet voor commerciële doeleinden gebruikt worden. De OPTA geeft aan dat ook hiervoor gewoon toestemming gevraagd dient te worden[19]. De genomen reactie hierop is als volgt:

"Per 5 juni 2012 is, als onderdeel van de Telecomwet, de Cookiewet van kracht. Deze stelt eisen aan het gebruik van cookies door websites.

De Rijksoverheid maakte tot dusver gebruik van cookies om hiermee de kwaliteit van de site verder te verbeteren. Na inwerkingtreding van de cookiewet is hiervan melding gemaakt op Rijksoverheid.nl. Naar het zich nu laat aanzien is deze melding niet voldoende om volledig aan de eisen van de cookiewet te voldoen.

De Rijksoverheid onderzoekt dit nader en bekijkt welke mogelijkheden er zijn voor structurele oplossingen. Tot een dergelijke oplossing is gerealiseerd zijn de cookies op Rijksoverheid.nl en Government.nl uitgezet. Ook voor de overige websites van de Rijksoverheid wordt geïnventariseerd of aanpassingen noodzakelijk zijn.

Voor de abonneeservice van Rijksoverheid.nl en Government.nl wordt een cookie weggeschreven die noodzakelijk is voor de werking van het abonneerproces. Het gaat hierbij om de cookie: _rijksoverheid_session. Doel van deze cookie is het beveiligen tegen cross site request forgery en het bewaren van de status tijdens het aanmelden, afmelden en wijzigen. Aan het eind van de sessie wordt deze cookie automatisch verwijderd." [20]

Er is dus nog veel onduidelijkheid welke naarmate de toekomst vordert naar verwachting zal afnemen. Wel zijn er al verschillende voorbeelden te vinden in Groot Brittannië die al wel voldoen aan de wetgeving. Deze is vergelijkbaar met de Nederlandse wetgeving behalve dat het in de Nederlandse

[18] www.rijksoverheid.nl *(Laatst geraadpleegd op 10-09-2012)*
[19] www.webwereld.nl/nieuws/111409/rijksoverheid-weigert-aan-cookiewet-te-voldoen.html *(Laatst geraadpleegd op 31-12-2012)*
[20] www.rijksoverheid.nl/cookies *(Laatst geraadpleegd op 10-09-2012)*

wetgeving niet duidelijk is of browser instellingen (Do-Not-Track[21]) voldoende zullen zijn of niet. Een Brits voorbeeld is de ICO die vraagt om toestemming en hierbij als ware een ja/nee manier gebruikt, ofwel wel of niet alle cookies accepteren. Een ander voorbeeld is British Telecommunications[22]. Deze website gebruikt een andere meer uitgebreide manier van toestemming vragen, namelijk met niveaus. Standaard is het niveau 'Strictly necessary & Performance' geselecteerd, wat inhoudt dat enkel cookies geplaatst worden om te onthouden welke producten er in het online winkelmandje van een bezoeker zitten en hoe ver de bezoeker is in het order proces. Dit is te vergelijken met technische cookies waarvoor geen toestemming gevraagd hoeft te worden. Het tweede niveau 'Functional' plaatst daarnaast cookies voor functionaliteiten als het onthouden van login gegevens, de website er consistent uit laten zien en live chat support. Het derde en laatste niveau wordt 'Targeting' genoemd. Hierbij worden connecties met social media aangeboden maar wordt informatie ook gedeeld met derden om relevante advertenties aan te kunnen bieden aan een bezoeker. De bezoeker heeft dus meer controle dan bij de ja/nee manier. Ook is er een pagina met alle details over de gebruikte cookies met naam, doel en aanbieder, dit valt onder de informatieplicht.

De opties ten behoeve van de gewijzigde wetgeving zijn momenteel dus de volgende drie:

- Informeren van de bezoeker over het gebruik (en niet volledig aan de wetgeving voldoen). *En:*
- Vragen van toestemming op de ja/nee manier. Of alle cookies of geen cookies, bij weigering kan de bezoeker de toegang tot de website ontzegd worden. *En/of:*
- Toestemming vragen door middel van meerdere niveaus. Hierbij heeft de bezoeker meer keuze en kan deze selecteren naar eigen inzicht.

Figuur 5.3 *"Opties ten behoeve van de gewijzigde wetgeving"*

5.1.1 Europese Unie

In de Europese Unie is er een onderling verschil tussen de leden qua implementatie van deze wet. Aangezien er een Europese richtlijn is, kan dit per lid anders geïmplementeerd worden in de landelijke wetgeving. In het ene land gebeurt dit op een strengere manier dan in het andere land. In Nederland is dit verhoudingsgewijs erg streng, zo blijkt ook uit het volgende:

"Vanwege de privacy online regelt het wetsvoorstel verder dat de consument beter moet worden geïnformeerd als er bestandjes -zogenaamde cookies- op zijn computer worden geplaatst. Daarbij moet de gebruiker zelf toestemming geven. De Tweede Kamer heeft deze bepaling aangescherpt, hoewel

[21] (DNT) Standaard voor browsers waarin de bezoeker aangeeft wel of geen toestemming te verlenen voor onder andere technieken als cookies.
[22] www.bt.com *(Laatst geraadpleegd op 31-12-2012)*

minister Verhagen dit als onnodig had ontraden. Hierdoor kunnen bedrijven in Nederland nadeel ondervinden ten opzichte van de rest van de Europese Unie."[23]

Dit nadeel uit zich in minder gebruik van cookies (aangezien toestemming vragen het aantal cookies met waardevolle gegevens aanzienlijk kan verminderen) en dus zijn er minder adequate (online) marketing doeleinden mogelijk. Andere landen hebben de wet op meerdere andere manieren geïmplementeerd. Zo is het informeren van de bezoeker en de mogelijkheid bieden om cookies te weigeren in sommige landen voldoende. Een andere optie is het verlenen van toestemming via de instellingen in de browser, ofwel wanneer de bezoeker cookies toestaat mogen deze door elke website (uitzonderingen daargelaten) geplaatst worden. Gezamenlijk wordt er wel gewerkt aan standaarden.

5.1.2 Standaarden

Het ontwikkelen van een standaard kan in veel gevallen uitkomst bieden, dit zou mogelijk kunnen zijn met zowel het informeren als toestemming vragen voor cookies. Wanneer bezoekers tijdens het bezoeken van websites mededelingen en toestemmingsvragen krijgen die totaal verschillend van elkaar zijn is dit inefficiënt. De bezoeker dient dan elk geval apart te bestuderen en te interpreteren en te verwerken. Zowel voor een aanbieder als ontvanger van informatie, in dit geval via een website, kunnen standaarden uitkomst bieden. Voor de aanbieder kan dan namelijk in samenwerking met andere organisaties een standaard ontwikkeld worden waarbij kennis en middelen gedeeld worden om zo tot een uitwerking te komen die de bezoeker zal herkennen. Een technisch voorbeeld van een standaard is opgesteld door W3C[24]. Hierdoor kunnen browsers de code (zoals HMTL, PHP) eenduidig interpreteren en de website goed weergeven. Deze standaard wordt nu wereldwijd gebruikt en gerespecteerd.

Behalve aan de voorkant kan een standaard ook bijdragen aan het achterliggende systeem. Bij het verwerken en opslaan van de toestemming zou zodoende profijt behaald kunnen worden door gebruik van een standaard. De toezichthouder kan op deze manier de standaard gemakkelijk controleren en de naleving van organisaties ook. Ditzelfde is het geval om de verwerking van persoonsgegevens te kunnen controleren.

Een dergelijke standaard kan op internationaal niveau ontwikkeld en gebruikt worden maar ook op nationaal niveau of per branche. Een voorbeeld van een internationale standaard is Do-Not-Track. Deze techniek zit verwerkt in de browser. Hiermee kan de bezoeker aangeven of websites wel of geen cookies mogen plaatsen op zijn randapparatuur. Dit is te vergelijken met het in Nederland gebruikte 'Bel-me-niet-register'[25]. Hierin kan een persoon aangeven niet gebeld te willen worden door organisaties voor aanbiedingen of promotiedoeleinden, dit wordt ook wel telemarketing genoemd. Ondanks een registratie hierin kan die persoon toch gebeld worden. Toezichtophouder OPTA zal hier dan op handhaven. Do-Not-Track werkt op dezelfde manier. Een persoon geeft in zijn browser aan geen cookies

[23] www.rijksoverheid.nl/nieuws/2011/06/22/vrij-internet-vastgelegd-in-telecomwet.html *(Laatst geraadpleegd op 31-12-2012)*
[24] The World Wide Web Consortium.
[25] Register waarin personen kunnen aangeven niet ongevraagd gebeld te willen worden door organisaties.

te willen ontvangen (opt-out). Desondanks kunnen hier ook alsnog ongewenst cookies geplaatst worden, de website is namelijk vrij in de interpretatie van deze wens van de bezoeker. Ook hier zal de toezichthouder op kunnen gaan handhaven. Net als bij andere standaarden zijn er bij de Do-Not-Track standaard enkele kenmerkende eigenschappen, zo blijkt ook uit (21): “Do-Not-Track is universeel geïmplementeerd, gemakkelijk in gebruik, te vinden en te begrijpen. Ook is het blijvend, effectief en afdwingbaar.”

Een standaard op nationaal niveau ligt daarnaast ook voor de hand. In Nederland is de interpretatie van de richtlijn uit de Europese Unie (6) streng overgenomen in de Nederlandse Telecommunicatiewet (1) waardoor een internationale standaard mogelijk niet zal voldoen. Bij het uitwerken van een nationale standaard kan naar voren komen dat een organisatie zich niet kan vinden in een standaard. Dit kan verschillende redenen hebben, zoals een eigen onderscheidende reputatie of een strakkere of lossere aanpak van de situatie. Dit blijkt in het geval van SNS Bank ook zo te zijn. Binnen SNS REAAL hebben de verschillende labels zoals SNS Bank, ASN Bank, RegioBank en Zwitserleven een eigen identiteit. Overal op gelijke wijze informeren en toestemming vragen kan niet even passend en doeltreffend zijn.

Organisaties kunnen ook onderling een standaard ontwikkelen binnen een eigen branche. In dit geval zou dit binnen de Nederlandse Vereniging van Banken kunnen. Hierbinnen zijn immers ook al richtlijnen te raadplegen voor het opstellen van het Privacy- en cookiereglement. Daarnaast kan er ook een standaard ontwikkeld worden door twee of meer organisaties onderling.

5.1.3 Vier banken

SNS Bank is één van de vier grotere banken die in Nederland actief is. Een standaard samen met de andere drie banken, te weten ABN AMRO, ING en de Rabobank zou een optie kunnen zijn. Bij een analyse van de vier banken blijken er overeenkomsten te vinden na een bezoek aan de startpagina van iedere bank (figuur 5.4). Dit is een momentopname en daarnaast informeren alle banken ook over cookies in het privacy- en cookiereglement (of een gelijksoortig document).

De manier waarop de bezoeker geïnformeerd wordt blijkt, op enkele kleine verschillen na, veelal gelijk. Alle vier hebben zij op de website een tekst over cookies. Na doorklikken hierop kent de essentie van de informatie ook veel overeenkomsten. Het is dus te stellen dat er een soort van standaard ontstaat, niet strikt, maar in een losse vorm. Een standaard kan dus, hetzij bewust of onbewust, ook in een lossere vorm ontstaan. Opvallend is dat de Rabobank als enige geen third party cookies plaatst. Gezien het feit dat deze al toestemming vraagt is dit wellicht een overweging en bewuste keuze.

Bank	Aantal cookies	Informeren	Toestemming vragen
ABN AMRO[26]	5 First party cookies	'Privacy en cookies' als tekst klein op iedere pagina (onderaan).	Nog niet gerealiseerd.
ING[27]	20 First party cookies 1 Third party cookie	'Cookies' als tekst klein op iedere pagina (onderaan). 'De ING en cookies' als nieuwsbericht.	Nog niet gerealiseerd.
Rabobank[28]	6 First party cookies	'Privacy en cookies' als tekst klein op iedere pagina (onderaan). 'Lees meer over cookies' in balk bovenaan.	Via balk bovenaan met de opties 'Cookies accepteren' of 'Cookies niet accepteren'.
SNS Bank[29]	20 First party cookies 4 Third party cookies	'Privacy en cookies' als tekst op iedere pagina onderaan in zijbalk.	Nog niet gerealiseerd.

Figuur 5.4 *"Informeren door vier Nederlandse banken"*

Bij het informeren en vooral bij het vragen van toestemming is de gebruiksvriendelijkheid erg belangrijk. De manier waarop dit gebeurt is dan ook veelal bepalend voor het wel of niet verkrijgen van toestemming maar daarnaast ook voor de perceptie van de bezoeker. Dit kan op verschillende manieren gerealiseerd worden.

5.1.4 De opties

Het is te stellen dat er enkele meest geschikte opties zijn voor het informeren en toestemming vragen. Figuur 5.5 geeft hier een overzicht van. Het informeren, toestemming vragen, toestemming verwerken in de website, toestemming opslaan en de verwerking (persoons)gegevens controleren/aantonen zijn de onderdelen die gerealiseerd dienen te worden. De manier waarop kan verschillen, evenals hoe dit weergegeven wordt. Bij elk onderdeel kunnen meerdere partijen betrokken zijn. In de volgende deelvraag zal de situatie voor SNS Bank uiteengezet worden.

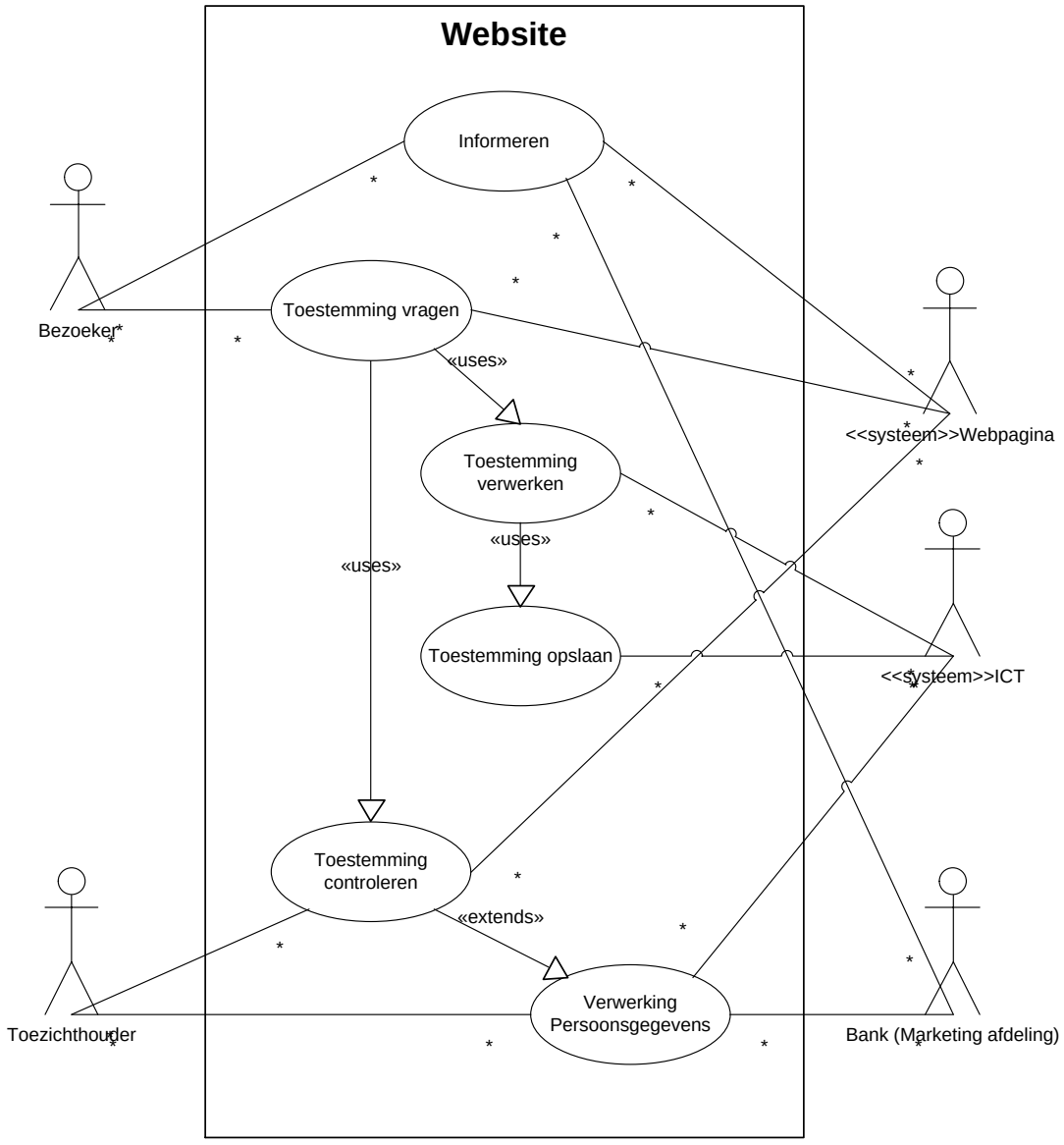
[26] Bij bezoek aan www.abnamro.nl
[27] Bij bezoek aan www.ing.nl
[28] Bij bezoek aan www.rabobank.nl
[29] Bij bezoek aan www.snsbank.nl

Onderdeel	Manier	Weergave	Partij
Informeren	- Kleine tekst - Privacy- cookiereglement - Als nieuwsbericht	- Via een balk op de website - Via een pop-up op de website	- Intern - In samenwerking - Derde partij
Toestemming vragen	- Geen toestemming vragen - Ja/Nee toestemming - Niveaus van toestemming - Via een ontwikkelde standaard	- Via een balk op de website - Via een pop-up op de website	- Intern - In samenwerking - Derde partij
Toestemming verwerken in website	- Eigen manier - Zelfde manier als andere organisaties - Via een ontwikkelde standaard	- Geen weergave	- Intern - Derde partij - Standaard
Toestemming opslaan	- Eigen manier - Zelfde manier als andere organisaties - Via een ontwikkelde standaard	- Geen weergave	- Intern - Derde partij - Toezichthouder
Verwerking (persoons)gegevens controleren/aantonen	- Eigen manier - Zelfde manier als andere organisaties - Via een ontwikkelde standaard	- Via eigen rapport - Via hetzelfde rapport als andere organisaties - Via standaard rapport	- Intern - Toezichthouder

Figuur 5.5 *"Opties voor informeren en toestemming vragen"*

5.2 Deelvraag 6: Waar dient de oplossing om de interactie tussen bank en bezoeker met cookies te ondersteunen aan te voldoen?

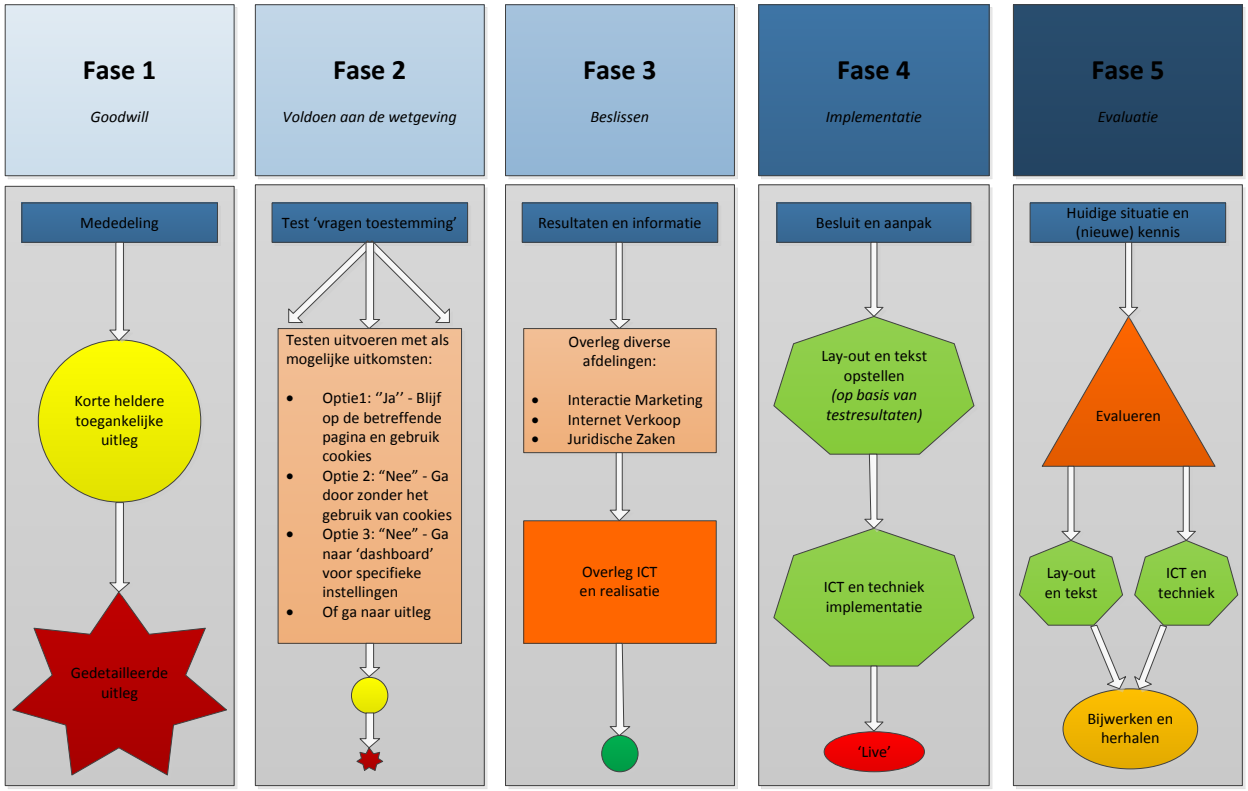
Het voldoen aan de vernieuwde wetgeving vereist veranderingen aan de ICT systemen binnen SNS Bank. De bezoekers van de website zullen dit merken, maar ook voor de bank zal er veel veranderen. Er zal omgegaan moeten worden met de nieuwe situatie en dit brengt uitdagingen met zich mee. De betrokken belanghebbenden, te weten bezoeker, toezichthouder en bank, zijn betrokken bij deze nieuwe situatie en zullen dit ondervinden in de onderlinge interactie. Ook zijn de systemen 'Webpagina' en 'ICT' te onderscheiden. De onderdelen waaraan voldaan dient te worden zijn weer te geven in relatie tot de belanghebbenden (figuur 5.6).



Figuur 5.6 *"Belanghebbenden use cases"*

5.2.1 Vijf fasen plan

Gegeven is dat er aan de wetgeving voldaan zal moeten worden. Hiervoor zijn meerdere opties mogelijk die invloed hebben op zowel de bezoeker als de bank. Hierin zal een afweging gemaakt moeten worden tussen gebruikersgemak en de wijze van informeren plus toestemming vragen. Op basis van het voorgaand is het vijf fasen plan opgesteld als weergegeven in figuur 5.7. Om tot een zo best passende oplossing te komen zijn enkele fasen te onderscheiden.

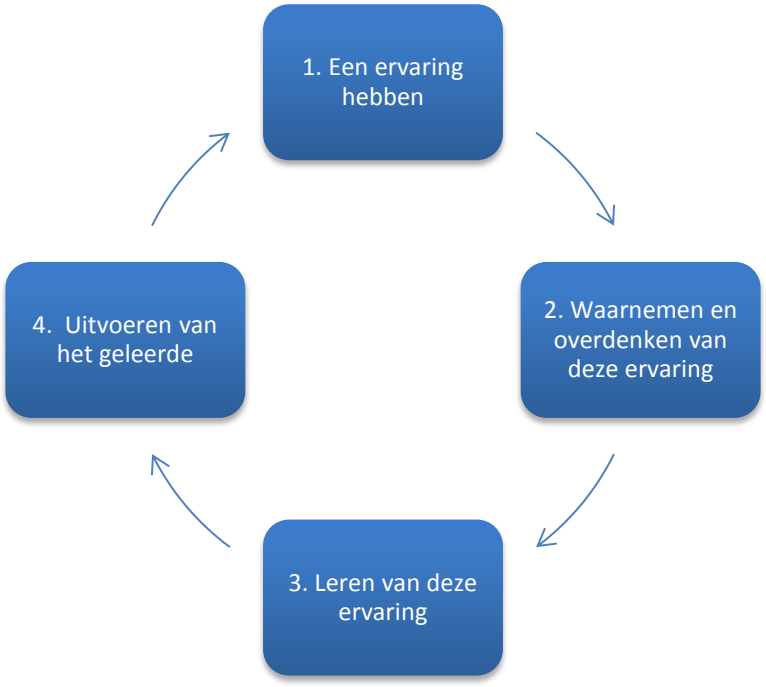


Figuur 5.7 *"Vijf fasen voor aanpak toestemming vragen voor cookies"*

De gewijzigde wetgeving, de perceptie van de bezoeker en de consequenties voor de belanghebbenden zijn gebaseerd op vertrouwen. Wanneer een bezoeker vertrouwen heeft in (de website van) SNS Bank zal hij eerder toestemming verlenen. Hoe hoger dit vertrouwen hoe meer kans op toestemming voor meer soorten cookies. Een andere factor is gebruikersgemak. Privacy en gebruikersgemak staan vaak tegenover elkaar. Wanneer een bezoeker meer gebruikersgemak wil kan hiervoor een deel van zijn privacy ingeleverd moeten worden. Het vertrouwen kan, gebaseerd op (22) en (4), in meerdere niveaus voorkomen, namelijk:

1. **“Doel-gebaseerd vertrouwen:** Vorm van vertrouwen waarbij twee of meer personen denken hetzelfde doel te hebben. Dit kan zowel een goed als slecht doel zijn. Propaganda en manipulatie kan dit soort vertrouwen versterken.
2. **Calculerend vertrouwen:** Vorm van vertrouwen waarbij een persoon de betrouwbaarheid van de ander probeert te berekenen/achterhalen door op zoek te gaan naar bewijs voor elkaars betrouwbaarheid. Ook wel een ‘utility-relation’.
3. **Kennis-gebaseerd vertrouwen:** Vorm van vertrouwen waarbij personen elkaar vertrouwen op basis van gebeurtenissen uit het verleden of door eerdere omgang. Meer een ‘friendship-relation’ dan ‘utility-relation’.
4. **Respect-gebaseerd vertrouwen:** Vorm van vertrouwen dat ontstaat en versterkt wordt op basis van respect tussen personen. Zij hebben overeenkomsten en zijn bereid om te overleggen en elkaar te begrijpen. Meest geschikte vorm voor betrouwbare personen.” (22) (4)

Het is dus zaak om een zo hoog mogelijk niveau van vertrouwen te bereiken. Naar (4) blijkt dat het vertrouwen voor gebruik van cookies kan voortvloeien uit een offline situatie. De aanzet kan bijvoorbeeld gegeven worden door de SNS Bank winkels, flyers of zichtbaarheid van SNS Bank als merk. Wanneer hier vertrouwen in is gevonden kan de bezoeker dit ook krijgen op de website. Personen zullen bij een bank eerder een hoger niveau van vertrouwen hebben dan bij bijvoorbeeld een webwinkel. Vertrouwen vloeit voort uit kennis, kennis wordt verkregen op basis van leren en ervaring. Naar (23), is er een leercyclus met vier stappen te onderscheiden (figuur 5.8). Per organisatie kan het niveau van vertrouwen verschillen, zoals weergegeven in figuur 3.11 zal het vertrouwen bij organisatie 2 hoger liggen dan bij organisatie 1.



Figuur 5.8 *“De vier stappen gebaseerd op de leercyclus”*

Er is dus een aanloopfase voordat een bezoeker kennis heeft van de situatie. Dit is vooral van toepassing bij het vragen van toestemming voor het plaatsen van cookies. Het niveau zal door de bezoeker ook constant bijgesteld worden op basis van nieuwe informatie en veranderingen. Hier dient rekening mee gehouden te worden in de situatie van SNS Bank. De bezoeker zal moeten weten wat cookies zijn of hier in ieder geval een beeld van vormen. Zowel met het informeren als toestemming vragen zal hij een ervaring hebben, deze overdenken, hiervan leren en vervolgens het geleerde uitproberen. Deze cyclus zal zich herhalen en zolang alles begrijpbaar en transparant is kan het niveau van vertrouwen stijgen.

Op basis van de voorgaande hoofdstukken en theorieën is het volgende plan opgesteld (figuur 5.7) met vijf fasen:

Fase 1

Gezien de tijd die nodig is voor een volledige implementatie kan gestart worden met een tijdelijke oplossing (deze voldoet nog niet volledig aan de wetgeving). Hierbij zal een mededeling geplaatst worden op de website om bezoekers bewust te maken van het feit dat er cookies gebruikt worden (steeds meer websites doen dit). Hiermee kan de bezoeker inzien dat hij al lange tijd cookies gebruikt en deze niet per se zijn privacy schaden. Dit kan iets zijn in de trant van “SNS Bank maakt gebruik van cookies om de website goed te laten werken en persoonlijk te maken. - Meer informatie”. Hiermee kan de bezoeker zijn perceptie met cookies veelal positief aanpassen en tevens wordt hiermee naar de buitenwereld, en de toezichthouder OPTA, het signaal afgegeven dat SNS Bank aan de implementatie werkt. Er zal ‘goodwill’ gekweekt worden en de bezoeker kan alvast de leercyclus doorlopen. Vanuit deze mededeling, welke ook weg geklikt kan worden, kan de bezoeker meer informatie bereiken. Dit kan in twee vervolgstappen, namelijk een heldere pagina met globale uitleg (ofwel ‘Blackbox’) en vervolgens een stap verder op een zakelijke pagina met alle details (ofwel ‘Whitebox’). Dit kan een tabel zijn met per cookie(soort) een toelichting en uitleg waarom deze gebruikt wordt. Dit is informatie die voor de uiteindelijke implementatie in ieder geval ook gerealiseerd moet worden.

Uit deze fase kunnen gegevens verkregen worden over de perceptie van de bezoeker ten opzichte van cookies. De bezoeker kan na doorklikken een mogelijkheid tot het uitschakelen van gebruik cookies (opt-out) geboden worden door middel van de bestaande functionaliteiten in de internet browser. In deze fase wordt getracht een vorm van vertrouwen bij de bezoeker te krijgen dat onder te brengen is in vertrouwensniveau 1 en deels 2. De stappen 1,2 en 3 van de leercyclus worden hierbij aangesproken.

Fase 2

Na de aanloopfase kan de volgende fase geïmplementeerd worden. Hierbij zal een mededeling op de website geplaatst worden die daadwerkelijk om toestemming vraagt alvorens er cookies geplaatst worden. De toestemming kan dan expliciet gegeven worden. Ook hier moet de mogelijkheid zijn tot meer informatie. Aan de hand van een test (meerdere soorten mededelingen en manieren, te bepalen met alle betrokken afdelingen) kan bepaald worden wanneer een bezoeker eerder toestemming zal geven, deze kan door fase 1 namelijk al een perceptie van cookies hebben ontwikkeld en zich in een niveau van vertrouwen bevinden. Wanneer de toestemming gegeven wordt zal de mededeling verdwijnen en komt de bezoeker terecht op de betreffende pagina van de website. Wanneer geen

toestemming gegeven wordt kan de bezoeker op een pagina met 'dashboard' komen met toelichting om deze alsnog te overtuigen of de mogelijkheid te geven om selectief cookies toe te staan (bijvoorbeeld wel inbound marketing van SNS Bank maar geen cookies van derden). Hieruit kunnen nuttige gegevens verzameld worden welke van belang zijn in de volgende fase. Als onderdeel van de wetgeving zal ook het privacy statement op de website vernieuwd moeten worden. Toestemming dient er gevraagd te worden op basis van de eigenschappen van cookies, bijvoorbeeld first party of third party cookies of tracking cookies, voor technische cookies hoeft geen toestemming gevraagd te worden. In deze fase wordt getracht de vorm van vertrouwen van de bezoeker zich verder te laten ontwikkelen naar vertrouwensniveau 3. Stap 4 van de leercyclus zal hierbij bereikt worden en op basis hiervan zal de leercyclus opnieuw doorlopen worden.

Fase 3

In deze fase zal de knoop doorgehakt worden. Een groot deel van de implementatie bestaat al en er wordt aan de wetgeving voldaan maar de uiteindelijke versie zal gerealiseerd worden in overleg met de betrokken afdelingen, aan de hand van het tijdsbestek, de te voeren strategie en de huidige situatie op het gebied van deze wetgeving en implementatie daarvan. Deze keuze moet vanuit marketing perspectief zo veel mogelijk toestemming opleveren, ofwel welke optie het beste uit de tests (uit fase 2) kwam, en vervolgens besproken worden met ICT wat betreft de uiteindelijke verdere mogelijkheden en benodigde tijd voor afrondende implementatie. Er is dan namelijk al veel bekend over de perceptie van de bezoeker, deze zal na de gewenning (of bewustwording) uit fase 1 en 2 ook gewijzigd zijn.

Deze fase bestaat dus uit het overleggen en gezamenlijk de optie selecteren welke het beste is voor de bezoeker en de organisatie. Dit houdt in dat SNS Bank voldoende bruikbare informatie kan verzamelen en de bezoeker de website op een vertrouwde en prettige manier kan bezoeken. In deze fase zal het vertrouwensniveau van de bezoeker vrijwel gelijk blijven of hij zal dit verder ontwikkelen door het leerproces. Hij kan na waarnemen, overdenken en leren tot een andere uitvoering komen. Bijvoorbeeld wel of geen toestemming geven voor bepaalde soorten cookies.

Fase 4

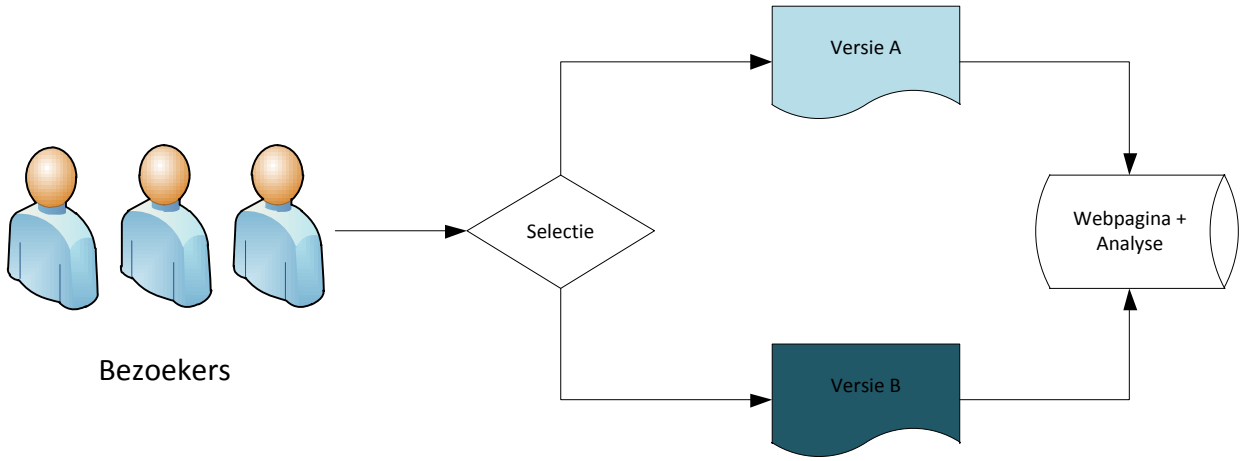
De uiteindelijke oplossing zal is samenwerking met Internet Verkoop bijgesteld worden qua tekst en lay-out waarna deze door ICT volledig technisch geïmplementeerd zal worden, dit gebaseerd op het resultaat van fase 3. Interactie Marketing heeft hierbij een adviserende rol. Omdat de uiteindelijke oplossing een variant zal zijn op een mogelijkheid uit fase 2 zal dit niet veel tijd kosten, veel werk is dan immers eerder al verzet. Wel zullen alle puntjes op de 'i' gezet moeten worden en dient de oplossing volledig aan de wetgeving te blijven voldoen. Een degelijke en onderhoudbare oplossing zal dan gerealiseerd zijn waarmee SNS Bank transparant en vertrouwd naar buiten kan treden en de toezichthouder tevreden zal zijn, evenals de bezoeker. De bezoeker heeft namelijk helderheid en voldoende informatie om zijn perceptie en vertrouwen te vormen. In deze en de volgende fase wordt getracht de vorm van vertrouwen naar het hoogste vertrouwensniveau te leiden. De gehele leercyclus is in dit geval doorlopen.

Fase 5

Deze laatste fase is die waarin het geheel geëvalueerd wordt. De oplossing kan dan bijgeschaafd worden en verder worden geoptimaliseerd aan de hand van nieuwe ontwikkelingen. Hierbij zijn de afdelingen op hun eigen gebied betrokken. Zowel de tekst en lay-out, als de perceptie van de bezoeker, de beschikbare technieken en mogelijkheden als de wetgeving kan namelijk veranderen. Op deze punten dient de oplossing met nog te bepalen criteria regelmatig getoetst te worden. Dit is een iteratief proces. De organisatie bevind zich vooral in deze, maar ook in eerdere fasen, zelf in de leercyclus.

5.2.2 Tests

Tests zullen uitwijzen welke manier voor SNS Bank het meest effectief is, ofwel een zo hoog mogelijk percentage toestemmingen (opt-in) oplevert. Zowel de tekst als lay-out is hiervoor bepalend gezien mogelijke wijzingen in de maatschappij, de perceptie van de bezoeker en wijzigingen in de wetgeving. Hiervoor is het van belang te analyseren hoeveel bezoekers toestemming verlenen en op basis waarvan. Dit kan getest worden op meerdere manieren, bijvoorbeeld de vraagstelling, de lay-out en het tijdstip. Hiervoor dienen geen cookies gebruikt te worden, welke een dergelijke test wel zuiverder kunnen maken. Wanneer het aantal verkregen toestemmingen vergeleken wordt met het aantal keer dat de toestemmingsvraag weergegeven wordt, wat de webserver kan bijhouden, kunnen analyse gegevens opgesteld worden. Een veel gebruikte testmanier hiervoor is een A/B test (figuur 5.9). Hierbij worden twee (of meerdere opties, dit wordt ook wel multivariate testen genoemd) aangeboden aan verschillende bezoekers, waarna zij doorgaan naar de webpagina waar zij naar op weg waren.



Figuur 5.9 *"A/B testen"*

De selectie wordt bepaald op basis van eigenschappen. Een mogelijkheid is de versies om en om weer te geven zodat er precieze controle is. Andere mogelijkheden zijn op basis van tijdstip of locatie van de bezoeker. Essentieel voor een correcte A/B test is dat deze selectie precies vast staat. Er dient namelijk

geen gebruik van cookies gemaakt te worden waardoor dat de enige houvast is. Bij veranderingen of een teruglopend aantal toestemmingen kan deze manier van testen uitkomst bieden. Een andere manier van testen is bezoekers enquêteren. Altijd is het de bedoeling om de bezoekers zo goed mogelijk te informeren en het liefst zoveel mogelijk toestemming te verkrijgen.

5.2.3 Requirements

In de ontwikkeling van de oplossing is het opstellen van requirements een belangrijk onderdeel. Hierbij kan nauwkeurig beschreven worden wat er mogelijk moet zijn in de nieuwe situatie en hoe vertrouwen (vier niveaus van vertrouwen) bij de bezoeker verkregen en behouden kan worden (leercyclus). Het dient als hulpmiddel om te communiceren tussen de marketing afdelingen en de ICT afdelingen. Er zijn drie soorten requirements te onderscheiden, namelijk:

- **Business requirement:** De 'Why'-vraag, waarom is er behoefte aan?
- **User requirement:** De 'What'-vraag, wat moet er mogelijk zijn?
- **System requirement:** De 'How'-vraag, hoe moet dit mogelijk zijn?

Alle drie de soorten bieden een dimensie aan die nodig is bij de ontwikkeling van een nieuw systeem. Samen vormen zij een beschrijving van de gehele oplossing. De requirements dienen altijd opgesteld te worden op basis van het S.M.A.R.T principe:

- **S:** specifiek
- **M:** meetbaar
- **A:** aanpasbaar
- **R:** realiseerbaar
- **T:** tijdgebonden

Echter stelt (24) dat 'T' niet voor tijdgebonden dient te staan bij het opstellen van requirements maar voor traceerbaarheid. Requirements zijn namelijk in veel gevallen afhankelijk van elkaar en traceerbaarheid is daarbij erg nuttig. Zo kan er namelijk een geheel beschreven worden waarbij onderlinge relaties zijn te onderscheiden.

Voor de beschrijving waar de oplossing[30] aan dient te voldoen zijn enkele tientallen requirements (zowel business, user en system requirements) opgesteld. Deze zijn te classificeren aan de hand van de MoSCoW methode. Deze manier van prioriteren is afhankelijk van de beschikbare middelen en tijd. Naar (25) zijn de volgende onderdelen te onderscheiden:

- **Must:** Een requirement welke geïmplementeerd dient te worden in de uiteindelijk oplossing voor dat de oplossing een succes genoemd mag worden.

[30] Een mogelijke uitwerking van de oplossing op basis van voorgaande informatie. Het betreft een voorstel waarvan de uiteindelijke oplossing kan afwijken.

- **Should:** Een requirement met hoge prioriteit welke indien mogelijk in de uiteindelijke oplossing bewerkstelligd dient te worden. Indien nodig kan deze requirement ook op andere manieren geïmplementeerd worden.
- **Could:** Een requirement welke wenselijk is maar niet strikt noodzakelijk. Alleen wanneer er genoeg beschikbare middelen en tijd beschikbaar is zal deze geïmplementeerd worden.
- **Won't:** Een requirement welke niet bewerkstelligd zal worden in de uiteindelijk oplossing maar wellicht wel in de toekomst. (25)

De requirements zullen herzien worden tot de belanghebbenden het eens zijn met de opgestelde requirements en bijbehorende MoSCoW prioritering (iteratief proces). De oplossing dient te voldoen aan de requirements in Appendix 'Requirements'. Deze requirements hangen veelal samen, de volgende requirements geven de onderdelen weer waaraan voldaan dient te worden:

Nr	Naam	Beschrijving	Prioriteit
Informeren en toestemming vragen:			
1	Bezoeker informeren op de website	De bezoeker dient bij het bezoeken van de website gelijk geïnformeerd te worden over welke categorieën cookies geplaatst worden en waarvoor deze gebruikt worden.	Must
6	Toestemming vragen aan de bezoeker	Bij een bezoek aan de website dient de bezoeker geïnformeerd te worden over het gebruik van cookies en zijn niveau van toestemming kunnen kiezen.	Must
Toestemming opslaan:			
11	Toestemming opslaan in cookie	Het niveau van de toestemming van de bezoeker dient vastgelegd te worden in een cookie op de randapparatuur van de bezoeker, opgeslagen dient te worden: een unieke code, toestemming voor welke categorie(n) en het tijdstip om zo te kunnen bewijzen dat de toestemming is verleend.	Must
12	Toestemming opslaan in database	Het niveau van de toestemming van de bezoeker dient vastgelegd te worden in een database, opgeslagen dient te worden: een unieke code, toestemming voor welke categorie(n) en het tijdstip om zo te kunnen bewijzen dat de toestemming is verleend.	Should

Toestemming verwerken:

13	Toestemming controleren	Bij een bezoek aan de website wordt gecontroleerd of de bezoeker toestemming heeft verleend en zo ja, het niveau van toestemming voor welke categorie(n) cookies.	Must
14	Toestemming verwerken	Bij een bezoek aan de website worden alleen de categorie(n) cookies geplaatst waarvoor door de bezoeker eerder toestemming is gegeven.	Must

Analyseren:

30	Analyse gegevens van tests	Analyse gegevens voor inzicht in de categorieën waarvoor bezoekers toestemming verlenen moeten beschikbaar zijn.	Must

Verwerking (persoons)gegevens controleren/aantonen:

31	Aantonen toestemming (bewijslast)	Altijd dient de toestemming van een bezoeker aangetoond te kunnen worden (bewijslast).	Must
32	Verwerking informatie inzichtelijk maken	De wetgeving vereist dat het verwerkingsproces van informatie door middel van cookies inzichtelijk is en duidelijk aan te tonen is dat de privacy van de bezoeker gerespecteerd wordt.	Must

Deze requirements, allen met de prioriteit ‘Must’ geven de basis weer waaraan de oplossing moet voldoen. Eén requirement heeft de prioriteit ‘Should’, deze is nodig voor het opslaan van toestemming in een database en later voor het aantonen van de toestemming (bewijslast). Deze requirement zal geïmplementeerd moeten worden vanwege de wetgeving maar dit kan desnoods in een later stadium gebeuren. De ‘tracability’ van deze requirements is ook van belang aangezien de oplossing daardoor specifiek beschreven wordt. Zie hiervoor de Appendix ‘Requirements’. De gehele oplossing bestaat dus uit het informeren via een duidelijke manier op de website, een scherm dat toestemming vraagt aan de bezoeker, wanneer de bezoeker geen toestemming geeft de opties om voor sommige cookies alsnog toestemming te geven, de optie om toestemming te wijzigen/intrekken, een achterliggend onderdeel dat de toestemming verwerkt en opslaat, de toepassing voor analyse doeleinden en een inzichtelijk proces wat kan bewijzen welke toestemming er door welke bezoeker wanneer is gegeven.

5.2.4 Corporate en labels

De oplossing heeft aanzienlijke impact op de gebruikerservaring. Naast het feit dat er een extra handeling uitgevoerd dient te worden (het toestemming geven) zal de reputatie van een organisatie beïnvloedt worden door de manier waarop de oplossing in de website en huidige ICT systemen wordt verwerkt. Iedere organisatie heeft een eigen identiteit. Bij de ene organisatie zal de bezoeker het eerder accepteren wanneer er minder transparant gecommuniceerd wordt dan de bij de ander. De ene zal op een andere manier toestemming vragen dan de ander en andere categorieën cookies hanteren. De manier van informeren en toestemming vragen dient te passen bij het imago dat de bezoeker verwacht. Dit is namelijk van invloed op de reputatie van de organisatie. Vooral bij banken is voorzichtigheid, integriteit en betrouwbaarheid van belang.

SNS REAAL wil voor alle labels transparant zijn en de verschillende labels hebben ieder een eigen identiteit, zo is ASN Bank gericht op duurzaamheid, RegioBank meer voor ouderen en bestemd voor het dorpse karakter en SNS Bank gericht op eenvoud in geldzaken. Laatstgenoemde zal dus op heldere en transparante wijze moeten communiceren. Op corporate niveau zou het voor de onderhoudbaarheid, efficiëntie en synergie effecten logischer zijn om voor alle labels dezelfde oplossing te hanteren, dit geeft schaalvoordelen. Dit is dus echter niet geheel mogelijk, misschien in grote lijnen, maar elk label zal zijn eigen identiteit in de oplossing moeten verwerken.

Kort gezegd zal de oplossing voor SNS Bank anders zijn dan voor die van de andere labels of organisaties. Dit vanwege de eigen identiteit maar ook de bestaande systemen die al in gebruik zijn. Vanzelfsprekend dient de oplossing hierbij te passen. De volgende deelvraag gaat hier verder op in.

5.3 Deelvraag 7: Welke aanpassingen dienen er gerealiseerd te worden binnen SNS Bank en welke invloed heeft dit?

De implementatie van de oplossing voor het 'cookievraagstuk' heeft impact op meerdere onderdelen, namelijk op de gebruikerservaring maar ook op de reputatie van SNS Bank, de ICT systemen en de bedrijfsvoering. Dit laatste is vooral afhankelijk van het aantal toestemmingen van bezoekers en voor welke soorten cookies. Er zullen onvermijdelijk aanpassingen plaatsvinden. Figuur 5.10 geeft de drie onderdelen weer waar verandering plaats zal vinden. Er is een samenhang te herkennen tussen deze onderdelen maar ook kennen zij ieder hun specifieke eigenschappen.

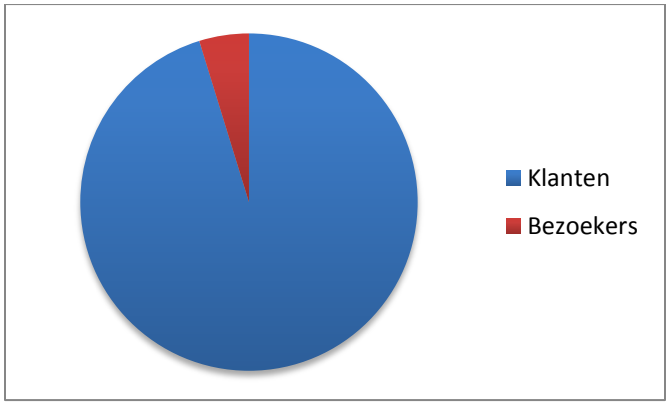
Figuur 5.10 *"Drie onderdelen waar verandering zal plaatsvinden"*

5.3.1 Toestemming vragen en inloggen

Het is gebleken dat de meest voor de hand liggende optie het vragen van toestemming is om cookies te kunnen plaatsen. Op deze wijze zal bij een voldoende aantal toestemmingen de bedrijfsvoering niet erg drastisch veranderen. In dat geval zijn er nog steeds gegevens beschikbaar voor het gebruik van de verschillende toepassingen. Hiervoor dient de website wel aanzienlijk aangepast te worden. Immers mogen er geen niet-technische cookies geplaatst en uitgelezen worden zonder dat hier vooraf toestemming voor is gegeven door de bezoeker. Ook de opslag en gegevensverwerking zal gewijzigd dienen te worden. Wanneer er weinig toestemming verkregen wordt zal de bedrijfsvoering en de soorten te gebruiken cookies ook wijzigen.

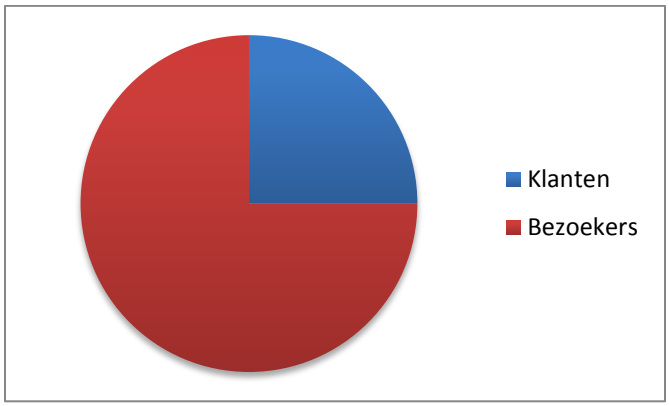
Een andere optie is het laten inloggen van klanten in plaats van het gebruik van cookies. Hier ontstaat een onderscheid tussen klant en bezoeker. Een klant kan namelijk wel inloggen en een bezoeker niet. De

klant heeft hierdoor meer controle en kan op deze wijze zelf beslissen zich bij bezoek aan het openbare deel van de website wel of niet kenbaar te maken. De website zal hiervoor minder ingrijpend aangepast hoeven te worden. Wel zal de gegevensverwerking en bedrijfsvoering aangepast worden. In dat geval is het namelijk meer verkopen en gebruikersgemak bieden aan bestaande klanten. Bij gebruik van cookies kunnen ook nieuwe klanten aangetrokken worden. Dit is één van de doelstellingen binnen veel organisaties, zo ook binnen SNS Bank. Uit gegevens in een willekeurige week[31] blijkt dat er *x* commerciële berichten aan klanten (ingelogd) worden getoond. Het aantal berichten dat aan bezoekers getoond werd is aanzienlijk kleiner, ongeveer twintig keer minder dan *x* (figuur 5.11).



Figuur 5.11 *"Verhouding weergaven commerciële berichten aan klanten en bezoekers"*

Naar gegevens blijkt ook dat het doorklikpercentage bij commerciële berichten aan ingelogde klanten lager is dan aan bezoekers (niet ingelogd). Stel dat *x* het doorklikpercentage van ingelogde klanten is dan is het doorklikpercentage van bezoekers ongeveer drie keer *x* (figuur 5.12). Het gebruik van cookies levert dus relatief gezien meer op dan de manier voor inloggen.



Figuur 5.12 *"Verhouding doorklikpercentage van klanten en bezoekers"*

[31] Interne weekrapportage enkel beschikbaar binnen SNS Bank.

Ondanks dat inloggen de bezoeker meer de controle geeft (‘user in control’) en ethische voordelen biedt is het gebruik van cookies in de huidige maatschappij effectiever. De volgende onderdelen zijn dan ook toegespitst op het gebruik van cookies, mede vanwege de omgeving waarin SNS Bank zich bevindt.

5.3.2 De website

De website is het onderdeel waarmee de bezoeker te maken heeft. Via dit communicatiekanaal kunnen cookies geplaatst en uitgelezen worden. Hier zal ook toestemming gevraagd moeten worden en een deel van de verwerking plaats dienen te vinden. Het informeren zal ook via de website verlopen. Kort gezegd dienen er informatiepagina’s te komen en het toestemming vragen dient in de lay-out van de website opgenomen te worden. Een keuze afdwingen bij de bezoeker zal het meest effectief zijn aangezien hij dan daadwerkelijk toestemming moet verlenen voor bepaalde cookies. Het is een optie om een balk op de website te plaatsen met de toestemmingsvraag waarbij de bezoeker de website zoals normaal kan gebruiken. Een pop-up waarin toestemming wordt gevraagd zal eerst doorlopen moeten worden voordat de website normaal gebruik kan worden. Hierbij wordt de bezoeker voor de keuze gesteld zodat gelijk duidelijkheid gegeven wordt en er daarna geen opvallende mededeling/vraag meer in beeld is. Hierbij kan hij kiezen om voor alle cookies toestemming te geven of voor bepaalde soorten. Een voor de hand liggende verdeling, welke SNS Bank ook gebruikt, zijn de volgende soorten cookies:

- Technische/functionele cookies *(geen toestemming vereist)*
- Anonieme analyse cookies
- Persoonlijke profielcookies
- Social media en advertenties *(ofwel derden)*

De website zal de toestemming (met eventueel voor welke soorten cookies) opslaan in een technische cookie op de randapparatuur van de bezoeker. Voor de bewijslast is een koppeling met achterliggende systemen tevens noodzakelijk. Voor elk apparaat (en elke browser) waarmee de bezoeker de website bezoekt zal toestemming gevraagd worden.

5.3.3 Opslag en gegevensverwerking

Vanuit de Nederlandse wetgeving dient de opslag van gegevens te voldoen aan een aantal vereisten en ook moet er bepaalde informatie opgeslagen worden. Zo kunnen opsporingsdiensten verzoeken tot de overhandiging van bepaalde gegevens, zoals IP-adressen van bezoekers. Dit staat los van de gegevens die opgeslagen dienen te worden voor het toestemming vragen. Aangezien de bewaartermijn vijf jaar is dient elk moment van toestemming specifiek opgeslagen te worden en minstens zo lang bewaard te blijven. Hierbij is het belangrijk dat zonder duidelijke communicatie in bijvoorbeeld het privacy- en cookiereglement, geen persoonsgegevens verwerkt mogen worden. Een aantal gegevens zijn vereist voor het aantonen aan de toezichthouder dat voor een specifieke cookie toestemming is verleent (figuur 5.13).

CookieID	Tijdstip	(KlantID)
Numerieke waarde	*Datum en tijd*	*Numerieke waarde*

Figuur 5.13 *"Gegevens voor verwerking toestemming"*

Daarnaast is het voor de situatie van SNS Bank gewenst om dit in het geval van een klant, te koppelen aan het KlantID. Hiermee kan het beheer van toestemming voor de klant gekoppeld worden aan zijn inlogomgeving. Hierdoor heeft hij meer controle over zijn eigen gegevens en kan de interactie tussen klant en de bank nauwkeuriger plaats vinden. Hiermee is echter wel een tot de persoon herleidbaar gegeven gemoeid. Dit dient in de voorwaarden (privacy- en cookiereglement) opgenomen te worden en ingezet te worden nadat de klant hiermee akkoord is gegaan. De klant kan in zijn inlogomgeving zelf kiezen of hij wel of geen commerciële berichten te zien wil krijgen. De Wbp is hierbij van toepassing en vanwege de omgekeerde bewijslast dient aangetoond te worden dat de gang van zaken aan de wetgeving voldoet. Dit kan met de opgeslagen gegevens en eventueel ook met de technische cookie die opgeslagen is op de randapparatuur van de bezoeker. De numerieke waarde kan ook verruild worden voor een categorie, bijvoorbeeld toestemming voor analyse cookies is niveau 2. Hiermee is dit een sleutel gekoppeld aan cookies die ingedeeld zijn in dit niveau (figuur 5.14) en dient de bezoeker herkend te worden aan een bezoekerID indien deze geen klant is. Dit is efficiënter in onderhoudbaarheid.

BezoekerID	Cookiecategorie	Tijdstip	(KlantID)
Numerieke waarde	***Numerieke waarde***	*Datum en tijd*	*Numerieke waarde*

Cookiecategorie	CookieID
Numerieke waarde	*Numerieke waarde*

Figuur 5.14 *"Koppeling bezoeker aan categorie met cookies voor verwerking toestemming"*

5.3.4 Bedrijfsvoering en soorten cookies

Door het vragen van toestemming zal de bedrijfsvoering wijzigen. De interactie tussen klant, bezoeker en bank kan een andere vorm aannemen. Wanneer iedere bezoeker toestemming verleent voor alle soorten cookies is de wijziging nihil. Echter is dit niet altijd even waarschijnlijk dus dient er rekening gehouden te worden met aanpassingen. Voor de bezoeker en klant is de grootste aanpassing het gevraagd worden om toestemming. Hierbij is het principe 'user in control' erg duidelijk te herkennen. Aan de kant van SNS Bank zijn er meerdere wijzigen te onderscheiden.

Momenteel gebruikt SNS Bank persoonlijke berichten voor diverse doeleinden. Wanneer dit niet meer, of in mindere mate mogelijk is, zal dit invloed hebben op andere bedrijfsmiddelen. Een voorbeeld is wanneer klanten bepaalde vragen hebben. Met een persoonlijk servicebericht kon dit voor de klant gelijk duidelijk zijn wanneer hij inlogt. Zonder deze functionaliteit zal de helpdesk veel vragen kunnen krijgen, iets wat zowel voor de klant als bank niet gewenst is. Het wel of niet gebruiken van soorten cookies heeft dus consequenties (figuur 5.15) maar ook kansen, bijvoorbeeld door te laten inloggen en

geen gebruik maken van cookies. Wanneer SNS Bank transparant is zal de reputatie kunnen verbeteren en de interactie tussen klant en bank inzichtelijker worden. Met deze bedrijfsvoering kan de interactie verbeteren wat tot tevreden klanten kan leiden en op deze wijze ook nieuwe klanten kan aantrekken.

De wijze van toestemming vragen blijft hierbij belangrijk. Naast dat dit transparant en zo gebruiksvriendelijk mogelijk dient te gebeuren is ook het moment van belang. Dit kan direct bij het bezoeken van de website maar ook op latere momenten. Bijvoorbeeld een bezoeker rustig laten rondkijken op de website en bij een volgende keer of later tijdstip pas om toestemming vragen. De eerste optie is echter gekozen vanwege eerder genoemde voordelen. Wel is het mogelijk om het verleende niveau van toestemming proberen te wijzigen naar toestemming voor meer soorten cookies. Op pagina's waar de bezoeker een klant wordt of een product aanvraagt kan dit voordeel opleveren voor beide partijen. Hetzelfde wanneer een pagina gebruikt maakt van bepaalde toepassingen die meer cookies vereisen, op dat moment kan de bezoeker gevraagd worden om hier toestemming voor te verlenen. Test zullen moeten uitwijzen welke momenten geschikt zijn en welke gerealiseerd kunnen worden.

Technische/functionele cookies

Toestemming vereist: Nee.

Doeleinden: Zorgen voor een goede werking van de website.

Bij uitschakeling:

De organisatie: De website werkt niet meer correct.
De bezoeker: Kan de website niet meer (geheel) correct bezoeken en sommige functionaliteiten zullen niet meer werken.

Voorbeeld: Cookies die de server zet om elke bezoeker de website te kunnen tonen.

Anonieme analyse cookies

Toestemming vereist: Ja.

Doeleinden: Hiermee kunnen statistieken op de website gemeten worden om zo de website te kunnen verbeteren en gebruiksvriendelijker te maken. Ook kunnen hiermee verschillende tests uitgevoerd worden.

Bij uitschakeling:

De organisatie: Zijn er geen statistieken beschikbaar en kan de website minder snel en doeltreffend geoptimaliseerd worden. Tests zijn in mindere mate mogelijk.
De bezoeker: Kan hierdoor de gewenste informatie minder snel vinden en de website kan

aanzienlijk minder gebruiksvriendelijk worden. **Voorbeeld:** Cookies van statistieken software als Google Analytics.
Persoonlijke profielcookies **Toestemming vereist:** Ja. **Doeleinden:** Hiermee kunnen profielen opgesteld worden van bezoekers om zo gerichte aanbiedingen en informatie te kunnen geven. **Bij uitschakeling:** **De organisatie:** Zijn er minder nauwkeurige profielen beschikbaar en kunnen er op de website (en andere communicatiekanalen) minder gerichte aanbiedingen gedaan worden. **De bezoeker:** Kan hierdoor irrelevante aanbiedingen krijgen, dubbele informatie te zien krijgen en niet persoonlijk benaderd worden. **Voorbeeld:** Cookies voor persoonlijke marketing doeleinden (inbound marketing).
Social media en advertenties **Toestemming vereist:** Ja. **Doeleinden:** Hiermee kunnen bezoekers herkend worden om zo gerichte advertenties te kunnen weergeven en verbindingen te leggen met social media. **Bij uitschakeling:** **De organisatie:** Bezoekers kunnen niet meer herkend worden en op websites kunnen er minder/geen gerichte advertenties weergegeven worden. Online conversie wordt zeer bemoeilijkt, net als retargeting. CTR[32] en CPS[33] kan niet meer (precies) bepaald worden waardoor samenwerking met derden minder of niet mogelijk kan zijn. **De bezoeker:** Kan hierdoor irrelevante en dubbele advertenties te zien krijgen. Ook is er geen integratie met social media mogelijk. **Voorbeeld:** Cookies van Doubleclick of Twitter/Facebook (of andere derden).

Figuur 5.15 *"Soorten cookies: doeleinden en consequenties bij uitschakeling"*

[32] Click through rate: percentage van het aantal keren doorgeklikt ten opzichte van het aantal weergaven van een advertentie. Op deze wijze kan het succes van een advertentie of campagne bepaalt worden.
[33] Cost per sale: de vergoeding die betaalt moet worden voor een verkoop of afsluiting van een product. Hiermee wordt uitgedrukt hoeveel kliks daadwerkelijk tot een aankoop leiden.

5.3.5 Overige aanpassingen

Er wordt gesproken over de website van de organisatie. Echter is er binnen een organisatie vaak meer dan één website te onderscheiden. Zo zijn er diverse websites voor bepaalde doelgroepen, campagnes in het verleden of actie pagina's. Het beheer hiervan ligt in sommige gevallen bij een andere partij. Voor cookies op deze websites dient ook toestemming gevraagd te worden. Hiervoor is een andere manier van beheer nodig of er dienen geen cookies of andere technieken, welke onder de Telecommunicatiewet vallen, gebruikt te worden.

Een ander belangrijk onderdeel is het gebruik van apps. Ook SNS Bank heeft een app beschikbaar voor haar klanten. Een app kan cookies plaatsen of gebruik maken van andere technieken als het uitlezen van een uniek nummer op een smartphone, tablet of andere randapparatuur. Net als voor de website dient hier ook toestemming voor gevraagd te worden. De manier van vragen en implementeren zal hier anders zijn. Mede vanwege het feit dat de techniek anders werkt kunnen sommige cookies wel of niet gebruikt worden maar ook vanwege de gebruikersinterface.

5.3.6 Ontwikkeling

De manier waarop gegevens verwerkt worden en de nodige aanpassingen zullen onderhoud met zich mee brengen. Zowel de cookies kunnen wijzigen qua indeling in soort als de wetgeving of de manier van bedrijfsvoering. Om enige houvast te hebben is een administratie van activiteiten, gebruikte cookies en analyse gegevens van belang. Hiervoor kunnen diverse hulpmiddelen ingezet worden. Aangezien het indelen van cookies ambigu kan zijn is de richtlijn (weergegeven in appendix 'Cookies indelen') als voorbeeld opgesteld.

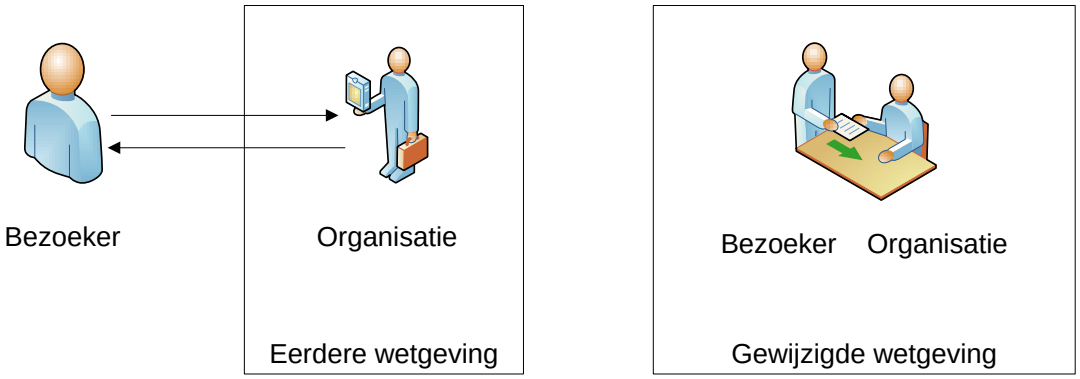
Een oplossing die, onafhankelijk van het soort randapparatuur, beheerd en ontwikkelt kan worden zal op de lange termijn uitkomst bieden. Een altijd accuraat overzicht van de gebruikte cookies, websites en andere communicatiekanalen met bijbehorende specificaties is daarnaast ook van belang. Dit komt ook terug in de Appendix 'Requirements'.

Met de ontwikkelingen, de requirements waar de mogelijke oplossing aan zou moeten voldoen en de uiteenzetting van de invloed van de veranderingen is een fundament gecreëerd voor het beantwoorden van de hoofdvraag. De uitwerking hiervan is de basis voor het volgende hoofdstuk.

6. CONCLUSIE

De mogelijkheden van technieken als cookies zijn uitvoerig uiteengezet, de eerdere en gewijzigde wetgeving is belicht evenals wat de ontwikkelingen in de omgeving zijn, waar de interactie tussen bank en bezoeker/klant aan dient te voldoen en welke aanpassingen er gerealiseerd dienen te worden. De omgeving is rijk aan factoren en gezien de situatie welke ook in het onderzoek benadrukt is, is te stellen dat er door de gewijzigde Telecommunicatiewet deels een grijs gebied is ontstaan. De manier waarop gegevensverzameling en verwerking lange tijd heeft plaatsgevonden zal veranderen. Voor welke gegevens en welke technieken dit precies geldt, is in sommige situaties niet eenduidig en kan aanzienlijke verwarring opleveren. Er kan namelijk een tegenstrijdigheid ontstaan op het punt van noodzakelijkheid. Wat de organisatie noodzakelijk acht kan voor de bezoeker niet zo zijn, dit is vooral het geval bij analyse cookies. De wetgeving is opgesteld vanuit het perspectief van de laatste belanghebbende, om zo de bezoeker meer controle geven over zijn privacy en op deze wijze het principe 'user in control' versterken.

In plaats van dat de organisatie meer bepaalt welke gegevens verkregen worden ligt dit nu meer bij de bezoeker. De wetgeving is nu een bescherming voor de gehele interactie. Figuur 6.1 geeft dit schematisch weer. Eerst was de wetgeving er onder andere om de organisatie een 'opt-out' te laten aanbieden, nu zal de bezoeker een 'opt-in' afgeven.

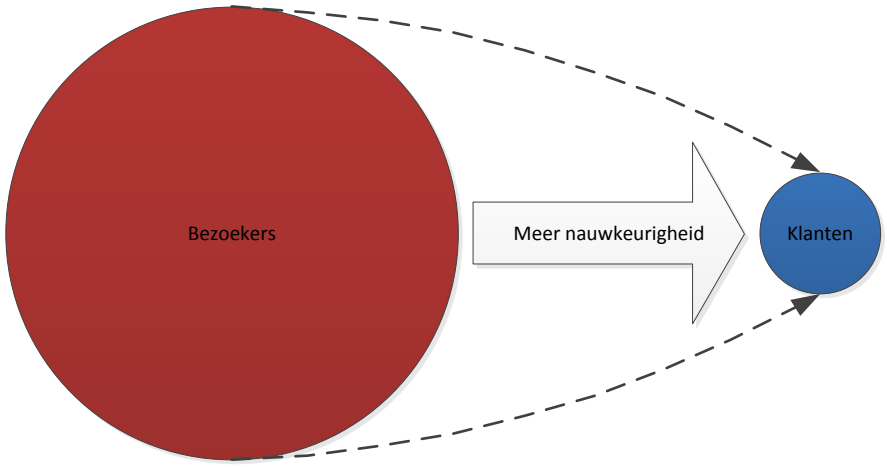


Figuur 6.1 *"Het verschil in wetgeving"*

Het niveau van vertrouwen is hierbij bepalend voor het wel of niet verlenen van toestemming in de vorm van een 'opt-in'. Doordat deze 'opt-in' te allen tijde gewijzigd dan wel ingetrokken moet kunnen worden ('opt-out') is belangrijk dat het niveau van vertrouwen behouden of verhoogd wordt. Dit wordt mede bepaald door de leercyclus die doorlopen zal worden. Wanneer er open en duidelijk geïnformeerd wordt over cookies en de bijbehorende doeleinden zal transparantie en vertrouwen bewerkstelligd worden. Dit vloeit uiteindelijk voort in een verbeterende reputatie van de organisatie.

Een nog duidelijkere situatie kan gerealiseerd worden door het laten inloggen van klanten. Groot voordeel hierbij is dat de gegevens die de organisatie ontvangt nog nauwkeuriger en dus waardevoller

zijn. De klant heeft zo nog meer controle en kan op deze wijze een zeer expliciete toestemming (soort 'opt-in') verlenen. Groot nadeel is hierbij het bereik van verkregen gegevens. De hoeveelheid is namelijk een stuk kleiner. In dit geval worden er namelijk enkel gegevens verwerkt van klanten en niet alle bezoekers (figuur 6.2).



Figuur 6.2 *"Meer nauwkeurigheid maar minder gegevens bij klanten ten opzichte van bezoekers"*

Techniek en marketing gaan vaak samen maar kunnen ook tegenstrijdig zijn. Vanuit marketing is het gewenst om binnen gestelde kaders als wetgeving, zo veel mogelijk precieze gegevens te verzamelen aangezien hiermee klanten beter bediend (service) kunnen worden en er meer bezoekers klant kunnen worden. De techniek staat hierbij als het ware in dienst van de bedrijfsvoering. In het geval van inloggen is dit precies te herkennen. Echter bij het vragen van toestemming worden door de wetgeving de technische mogelijkheden beperkt. Er ontstaat een onderlinge tegenstrijdigheid tussen zoveel mogelijk gegevens verkrijgen of nauwkeurigere gegevens. Welke manier geschikter is, is afhankelijk van de situatie waarin de organisatie zich bevindt en welk soort doelgroep deze heeft. Op basis van de voorgaande hoofdstukken zijn er drie mogelijkheden met voor- en nadelen te onderscheiden (figuur 6.3).

1. Niet voldoen	2. Toestemming vragen	3. Inloggen
Situatie waarbij de organisatie de huidige bedrijfsvoering en gebruik van bestaande technieken blijft voortzetten.	**Situatie waarbij de organisatie toestemming vraagt aan de bezoeker voor het gebruik van cookies.**	**Situatie waarbij de organisatie enkel gegevens verkrijgt van klanten na inloggen.** (Toestemming voor verwerking persoonsgegevens al verkregen in de voorwaarden)
+ Veel gegevens verkrijgen + Winst kan hoog zijn + Geen aanpassingen nodig	+ Meer transparantie + Reputatie verbeterd + Bezoeker en klant serieus nemen + Geen hoge boetes	+ Preciezere gegevens + Bezoeker en klant serieus nemen + Meer transparantie + Reputatie verbeterd + Geen hoge boetes
- Reputatie verslechterd - Hoge boetes toezichthouder - Bezoeker misleiden	- Minder gegevens verkrijgen - Aanpassingen nodig - Gebruiksvriendelijkheid kan dalen	- (Veel) minder gegevens verkrijgen - Aanpassingen nodig - Langere aanlooptijd

Figuur 6.3 *"Overzicht opties met voor- en nadelen"*

Niet voldoen aan de wetgeving is een optie voor bedrijven (veelal buiten Nederland) die het winstmodel kunnen blijven behouden met een slechtere reputatie en de hoge boetes. Voor vrijwel alle organisaties is dit geen reële optie. Toestemming vragen is gezien de omgeving en huidige maatschappij de meest doeltreffende optie. Hierbij zijn echter veel aanpassingen nodig en dient het toestemming vragen gebruiksvriendelijk in de website verwerkt te worden. Inloggen is een goede optie gezien vanuit de klant, voor de organisatie is een groot nadeel dat hierbij veel minder gegevens worden verkregen. Het werven van nieuwe klanten is hierbij niet meer iets wat de organisatie in eigen handen heeft, bij de andere opties is dit wel het geval. De reden hiervoor is dat de klant waardering moet krijgen voor de transparante manier waarop de organisatie omgaat met gegevens. Na een langere aanlooptijd kan dit zorgen voor een meer gewaardeerde organisatie met een groeiend aantal klanten. Dit is in de huidige informatie consumerende maatschappij echter nog een meer ideële optie.

6.1 Hoofdvraag

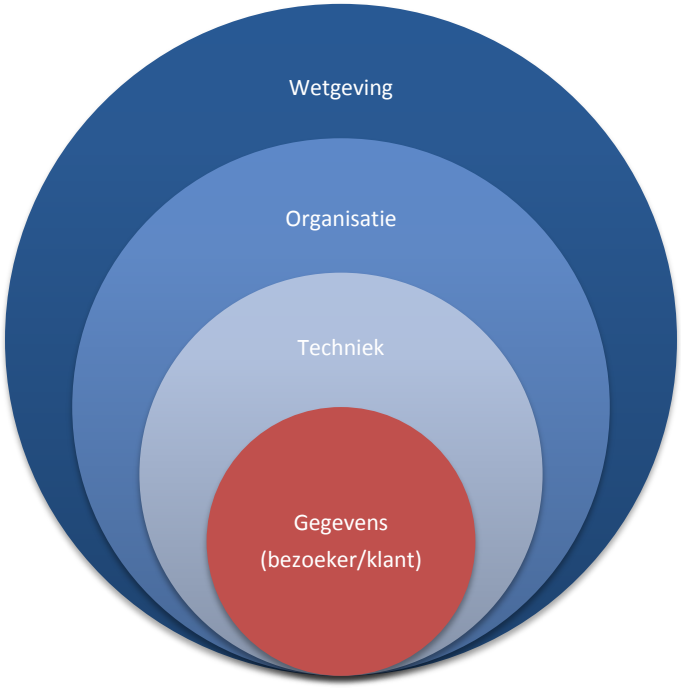
Het verrichte onderzoek in voorgaande hoofdstukken is noodzakelijk voor een onderbouwde beantwoording van de hoofdvraag. Op basis hiervan kan nu de hoofdvraag beantwoord worden:

Welke veranderingen dienen er plaats te vinden binnen SNS Bank om te voldoen aan de gewijzigde wetgeving en wat is hierbij de impact op de gebruikerservaring?

Het is duidelijk dat SNS Bank, net als vele andere organisaties, gebruik maakt van cookies. Ook is geconstateerd dat hierbij gebruik wordt gemaakt van meerdere soorten cookies, te weten: technische-cookies, analyse cookies, profielcookies en social media/advertentie cookies. Na uiteenzetting van de gewijzigde Telecommunicatiewet blijkt dat deze geheel van toepassing is, zowel gezien het eerste deel (toestemming vragen) als het tweede deel (verwerking van persoonsgegevens). De bedrijfsvoering is ingericht op de beschikbare gegevens en opgebouwde profielen. Ook sommige betalingen aan derden zijn hierop gebaseerd. Ofwel de organisatie is in overeenstemming met de techniek.

SNS Bank is een organisatie die haar bezoeker en klant serieus neemt. Hierbij is transparantie erg belangrijk. Naar de missie en visie blijkt daarnaast dat klanten zelf bepalen hoe, waar en wanneer ze hun geldzaken regelen. In deze reeks past ook het behouden van de menselijke maat in geldzaken en het begrip 'user in control'. Een heldere uitleg naar de klanten en bezoekers over het gebruik van cookies en de gebruikte doeleinden zou daarom het meest geschikt zijn, aangezien pas na toestemming cookies gebruikt worden. Daarnaast zal de reputatie met een heldere transparante informatievoorziening verder kunnen verbeteren. Optie twee, het toestemming vragen is daarom het meest geschikt. Het enkel gebruiken van inloggen (optie drie) zal in de huidige maatschappij met andere concurrenten en organisaties verhoudingsgewijs erg weinig gegevens opleveren. Een combinatie van optie twee en optie drie kan wellicht in een later stadium uitkomst bieden om meer voordelen te behalen.

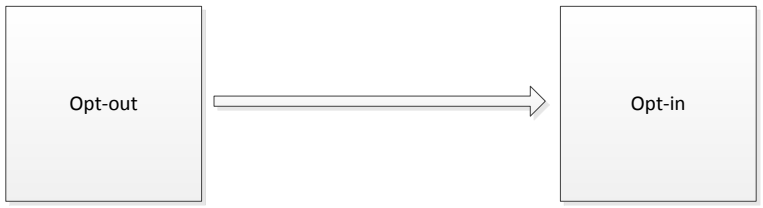
Om dit te bewerkstelligen dienen er meerdere aanpassingen plaats te vinden. De eerdere requirements gaven dit al aan. Het belangrijkste is geen niet-technische cookies plaatsen totdat de bezoeker hier toestemming voor heeft gegeven. Hiermee is het wetsaspect vervuld. Hiervoor zijn aanpassingen in de techniek nodig. Deze techniek hangt samen met de organisatie, ook wel bedrijfsvoering. Dit onderdeel hangt weer direct samen met de wetgeving (figuur 6.4).



Figuur 6.4 *"De bezoeker ten opzichte van wetgeving, organisatie en techniek"*

De wetgeving is in de vorm van de gewijzigde Telecommunicatiewet vastgesteld, ofwel de aanleiding. Hierop gebaseerd zal de organisatie veranderingen doorvoeren in de bedrijfsvoering. Zo zal er rekening gehouden moeten worden met de verandering in de hoeveelheid van gegevens, immers pas gegevens

verzamelen na het verkrijgen van toestemming zal naar verwachting minder gegevens opleveren dan in de eerdere situatie. Wellicht kunnen de bedrijfsprocessen op slimme wijze aangepast worden op deze situatie, bijvoorbeeld door gegevens te zien als een steekproef van het geheel. Door de gestelde wetgeving zullen de organisatie en techniek onderling synergie moeten behalen om zo de klant en de bezoeker dienstverlening te kunnen bieden, de grens hiertussen zal vervagen. Tevens moet de organisatie haar doelen kunnen behalen. De kern van verandering is de overgang van een opt-out naar een opt-in (figuur 6.5).



Figuur 6.5 *"Van opt-out naar opt-in"*

Om te voldoen aan de gewijzigde wetgeving is er in ieder geval aanpassing nodig op de website en achterliggende ICT systemen. Er moet geïnformeerd worden over cookies, toestemming gevraagd worden en dit alles in een inzichtelijk transparant gemaakt proces. De achterliggende systemen moeten dit verwerken zoals beschreven in het vorige hoofdstuk. De bedrijfsvoering dient hiermee in overeenstemming te zijn. De requirements hebben hier al een precies beeld in gegeven. Figuur 6.6 geeft hiervan een globale uiteenzetting.

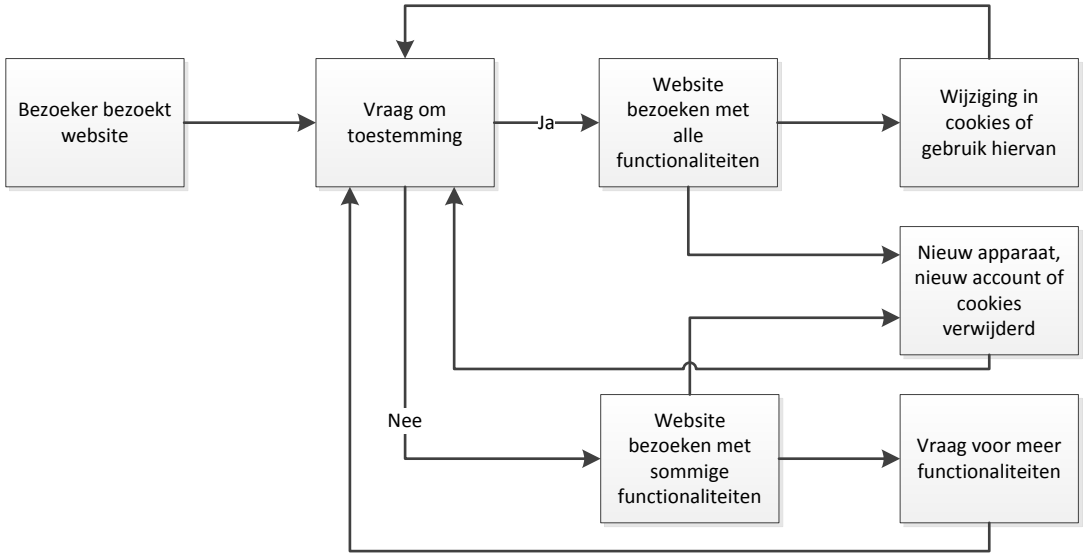
Eerdere situatie	Gewijzigde situatie
Veel cookies zonder overzicht en wellicht ongebruikt.	Alleen nodige cookies in gebruik met een nauwkeurig bijgehouden overzicht.
Alle cookies plaatsen bij bezoeker.	Toestemming vragen voor cookies, alleen de cookies waarvoor toestemming is gegeven plaatsen.
Veel gegevens beschikbaar.	Minder gegevens beschikbaar, slimmer omgaan met gegevens.
Opslag van geplaatste cookies niet nodig.	Opslag van geplaatste cookies is noodzakelijk voor de bewijslast, dus toestemming met bijbehorende eisen.
Bedrijfsonderdelen kunnen bestaan door vele gegevens.	Bedrijfsonderdelen dienen efficiënter ingedeeld te worden vanwege minder gegevens.
Mogelijkheid tot niet meer plaatsen van cookies (opt-out).	Mogelijkheid tot niet plaatsen van cookies tot toestemming is verleend (opt-in).

Figuur 6.6 *"Benodigde aanpassingen"*

De bezoeker/klant communiceert via de techniek met de organisatie. Deze manier van online interactie zal veranderen in de nieuwe situatie. Gebruikersgemak is hierbij een belangrijk onderdeel maar ook een indicator. Tegenwoordig zijn bezoekers bereidwillig om gegevens prijs te geven wanneer dit meer gebruikersgemak oplevert. Hierbij is het behouden van controle van groot belang. In de nieuwe situatie zal de bezoeker/klant bereid kunnen zijn om gegevens prijs te geven, en dus cookies toe te staan, wanneer hij hier gerichte serviceberichten of aanbiedingen voor terug krijgt. Gebleken is dat het niveau van vertrouwen verschillend is per situatie. Het te doorlopen proces op de gebruikerservaring is weergegeven in figuur 6.7. Voorafgaand aan de gewijzigde wetgeving bezocht een bezoeker de website en kreeg gelijk de website met alle functionaliteiten. In de gewijzigde situatie zal toestemming moeten worden gegeven of toestemming voor bepaalde soorten cookies, en dit gebeurt gelijk bij bezoek van de website. Wanneer een bezoeker toestemming heeft gegeven zal hij een tijd geen toestemmingsvraag meer zien, tenzij:

- De toestemmingscookies verwijderd worden, hetzij met of zonder opzet.
- Er andere randapparatuur gebruikt wordt om de website te bezoeken.
- De browser (of het besturingssysteem op de randapparatuur) opnieuw geïnstalleerd is.
- De organisatie graag toestemming van de bezoeker wil voor meer soorten cookies en de vraag voor toestemming op bepaalde momenten nogmaals zal stellen.

De vraag voor toestemming zal in de praktijk meerdere malen voorkomen. Het effect op gebruikerservaring, in veelal negatieve vorm, zal hierdoor toenemen.



Figuur 6.7 *"Proces gebruikerservaring"*

Terugkomend op de situatie in figuur 4.4 is met weging van de impact op online interactie de meer gewenste situatie weergegeven in figuur 6.8. Hierbij is het gebied waarvoor de wetgeving daadwerkelijk

bedoeld is vrijwel bedekt in plaats van overregulering. De bezoeker is hierbij beschermt en door dit kleine 'overblijvende' gebied is een situatieafhankelijke beoordeling mogelijk. Hierdoor blijft innovatie voor organisaties te realiseren en kan de ontwikkeling van persoonlijke technieken en websites blijven bestaan. Of deze situatie er zal komen zal blijken in de toekomst.

Figuur 6.8 *"Gewijzigde wetgeving met nuance"*

Evaluatie van de manier van toestemming vragen en eventuele nieuwe wetswijzigingen zal zorgen voor een efficiënte transparante organisatie die haar bedrijfsmiddelen zodanig blijft inzetten dat zowel de organisatie als bezoeker (verbeterende gebruikerservaring) hier baat bij hebben.

6.2 Toekomst

De gewijzigde Telecommunicatiewet heeft aanzienlijke impact op de gebruikerservaring en op organisaties, waaronder SNS Bank. Naast de technische aanpassingen zal de bedrijfsvoering ook veranderingen door moeten voeren. Voordeel hierbij is bijvoorbeeld dat organisaties gecontroleerd gaan kijken naar wat wel en niet nodig is en waarvoor. Hierbij wordt als het ware een evaluatie afgedwongen zodat bedrijfsmiddelen en de bedrijfsvoering efficiënter kunnen worden. Hierbij zal een beter onderhoudbaar proces ontstaan wat voorbereid is op de toekomst.

Wat al eerder naar voren kwam is dat de overregulering van de gewijzigde wetgeving een andere wending lijkt te krijgen. De minister van Economische Zaken heeft een brief geschreven waarin hij kortgezegd pleit voor het mogen plaatsen van analyse cookies zonder dat hiervoor toestemming nodig is (26). Hierbij moet wel aan voorwaarden voldaan worden zoals dat de analyse cookie een first party cookie dient te zijn en gegevens niet met andere partijen gedeeld mogen worden. Dit zal de impact op online interactie kunnen stroomlijnen en de negatieve impact op de gebruikerservaring verkleinen. De precieze uitwerking zal nog onderzocht moeten worden.

Een mogelijke ontwikkeling geschikt voor aanvullend onderzoek is de verschuiving naar andere technieken. Doordat het gebruik van cookies zichtbaar is voor de bezoeker kan bijvoorbeeld overgestapt worden naar andere technieken die niet waar te nemen zijn voor de bezoeker maar waar juridisch

gezien ook toestemming voor gevraagd dient te worden. Dit is geen onrealistische, hetzij niet ethische, ontwikkeling. Ook is vooral ingegaan op het eerste deel van de gewijzigde wetgeving (toestemming vragen). Onderzoek naar hoe IT ondersteuning kan geven bij het tweede deel (omgekeerde bewijslast) kan veel organisaties helpen.

De vraag voor toestemming kan vanwege de impact op de gebruikerservaring dusdanige invloed hebben dat bezoekers hier geen aandacht meer aan willen besteden en het in plaats van voordeel (control) als nadeel gaan zien. Een soort standaard die ingesteld kan worden om altijd toestemming te geven voor alle cookies, of bepaalde soorten, is dan ook niet ondenkbaar. Ook bezoekers die hun cookies na een sessie zelf wissen kunnen hier baat bij hebben. Hoe een dergelijke standaard eruit moet zien en technisch plus juridisch geïmplementeerd kan worden is interessant voor vervolgonderzoek.

Daarnaast roept de invoering van de gewijzigde wetgeving een tegenstelling op. In het ‘offline leven’ worden namelijk steeds meer gegevens verzameld van personen. Bijvoorbeeld bij een bezoek aan winkel of openbare gebieden. Het aantal camera’s neemt hier steeds meer toe. In het ‘online leven’ wil men de bezoeker met deze wetgeving meer beschermen terwijl in het ‘offline leven’ dus het tegenovergestelde gebeurd. Hoe dit zich ten opzichte van elkaar verhoudt en elkaar beïnvloedt kan interessante resultaten opleveren.

Het is in ieder geval duidelijk dat het speelveld tussen privacy, gebruikersgemak en marketing continu van elkaar afhankelijk is en zal blijven veranderen.

7. BIBLIOGRAFIE

Overzicht van gebruikte literatuur en andere bronnen.

1. *Wijziging van de Telecommunicatiewet ter implementatie van de herziene telecommunicatierichtlijnen.* **Staten-Generaal, Eerste Kamer der.** 32 549, Nederland : Vergaderjaar 2010-2011, 2010.

2. *Jaarverslag 2011.* **REAAL, SNS.** 2012.

3. *The ontological interpretation of informational privacy.* **Floridi, Luciano.** Bari, Italy : Ethics and Information Technology (2005) 7: 185–200, Springer, 2006.

4. *Online & offline privacy.* **Wolfkamp, Niek.** Bachelorscriptie, Nederland : Radboud Universiteit Nijmegen, 2011.

5. *Privacy, emotional closeness, and openness in cyberspace.* **Ben-Ze'ev, Aaron.** Israel : Department of Philosophy, University of Haifa, Israel, Computers in Human Behavior 19 (2003) 451–467, Elsevier Science Ltd, 2003.

6. *Directive 2002/58/EC of the European Parliament and of the council.* **European Union, The European Parliament and of the council of the.** European Union : Official Journal of the European Communities, 31-07-2002.

7. *Is Privacy Relative?* **Räikkä, Juha.** sl : Journal of social Philosophy, Vol. 39 No. 4, Winter 2008, 534–546, Wiley Periodicals, Inc, pp. 534–546, 2008.

8. *Privacy and the Limits of Law.* **Gavison, Ruth.** sl : The Yale Law Journal, Vol. 89, No. 3 (Jan., 1980), pp. 421-471, 1980.

9. *The right to privacy.* **Warren, Samuel D. en Brandeis, Louis D.** sl : Harvard Law Review, Vol. 4, No. 5 (Dec. 15, 1890), pp. 193-220, The Harvard Law Review Association, 1890.

10. *A bite too big: Dilemma's bij de implementatie van de Cookiewet in Nederland.* **Linda Kool, Arjanna van der Plas (TNO), Nico van Eijk, Natali Helberger, Bart van der Sloot (IViR).** Delft : TNO, 2011.

11. *HTTP Cookies: Standards, Privacy, and Politics.* **Kristol, David M.** sl : Lucent Technologies, February 1, 2008 cookie.tex 3.11 appendix.texx 3.2 cookie.bib 3.4, 2001.

12. *How Unique Is Your Web Browser?* **Eckersley, Peter.** sl : Electronic Frontier Foundation, Vol. Lecture Notes in Computer Science, 2010, Volume 6205/2010, 1-18,.

13. *HTTP State Management Mechanism RFC 6265.* **A. Barth, U.C. Berkeley.** Standards Track, sl : Internet Engineering Task Force , April 2011.

14. *A Survey of Cookie Management Functionality and Usability in Web Browsers.* **Yee, Ka-Ping.** University of California, Berkeley : sn, 2002.

15. *Cookiewet aangenomen door de Eerste Kamer.* **Juridische Zaken, SNS REAAL.** Utrecht : Intern, Mei 2012.

16. *Opinion on data protection issues related to search engines.* **Directorate C (Civil Justice, Rights and Citizenship) of the European Commission.** Article 29 Data protection working party, Brussel : 00737/EN, 2008.

17. *Flash Cookies and Privacy.* **Ashkan Soltani, Shannon Canty, Quentin Mayo, Lauren Thomas, Chris Jay Hoofnagle.** Berkeley : University of California, 2009.

18. *The EU E-Privacy Directive: A Monstrous Attempt to Starve the Cookie Monster?* Frederic Debusseré : International Journal of Law and Information Technology Vol. 13 No. 1 Oxford University Press, 2005.

19. *Gedragscode Verwerking Persoonsgegevens Financiële Instellingen.* **verzekeraars, Nederlandse Vereniging van Banken (NVB) en Verbond van.** rapportnummer: 2010/bl/13170/mblom, 16 maart 2010.

20. *Verslag OPTA rondetafelbijeenkomst cookiewetgeving.* **OPTA.** Nederland : In samenwerking met DDMA en IAB, 2012.

21. **Hannes Tschofenig, Rob van Eijk.** *Do Not Track, An Attempt to Frame the Debate.* Princeton, NJ, USA : W3C Workshop on Web Tracking and User Privacy, 2011.

22. **Koehn, Daryl.** *The Nature of and Conditions for Online Trust.* Houston, U.S.A. : Journal of Business Ethics 43: 3–19, 2003. Kluwer Academic Publishers, 2003.

23. **Kolb, Alice Y. en Kolb, David A.** *Learning Styles and Learning Spaces: Enhancing Experiential Learning in Higher Education.* sl : Academy of Management Learning & Education, 2005, Vol. 4, No. 2, 193–212, 2005.

24. **Mike Mannion, Barry Keepence.** *SMART Requirements.* United Kingdom : Software Engineering Research Group. Napier University. Notes vol 20 no 2, 1995.

25. **Iba, Kevin Brennan.** *A guide to the Business Analysis Body of Knowledge (BABOK guide), version 2.0.* Toronto, Ontario, Canada : International Institute of Business Analysis, 2009.

26. **Kamp, Minister van Economische Zaken H.G.J.** *Analytische cookies en artikel 11.7a van de Telecommunicatiewet. '*s-Gravenhage : Directoraat-generaal Energie, Telecom & Mededinging Directie Telecommarkt, 20 december 2012.

8. APPENDIX

In deze scriptie is diverse informatie en data gebruikt. Een overzicht daarvan is te vinden in dit hoofdstuk. Een deel hiervan is alleen beschikbaar binnen SNS Bank.

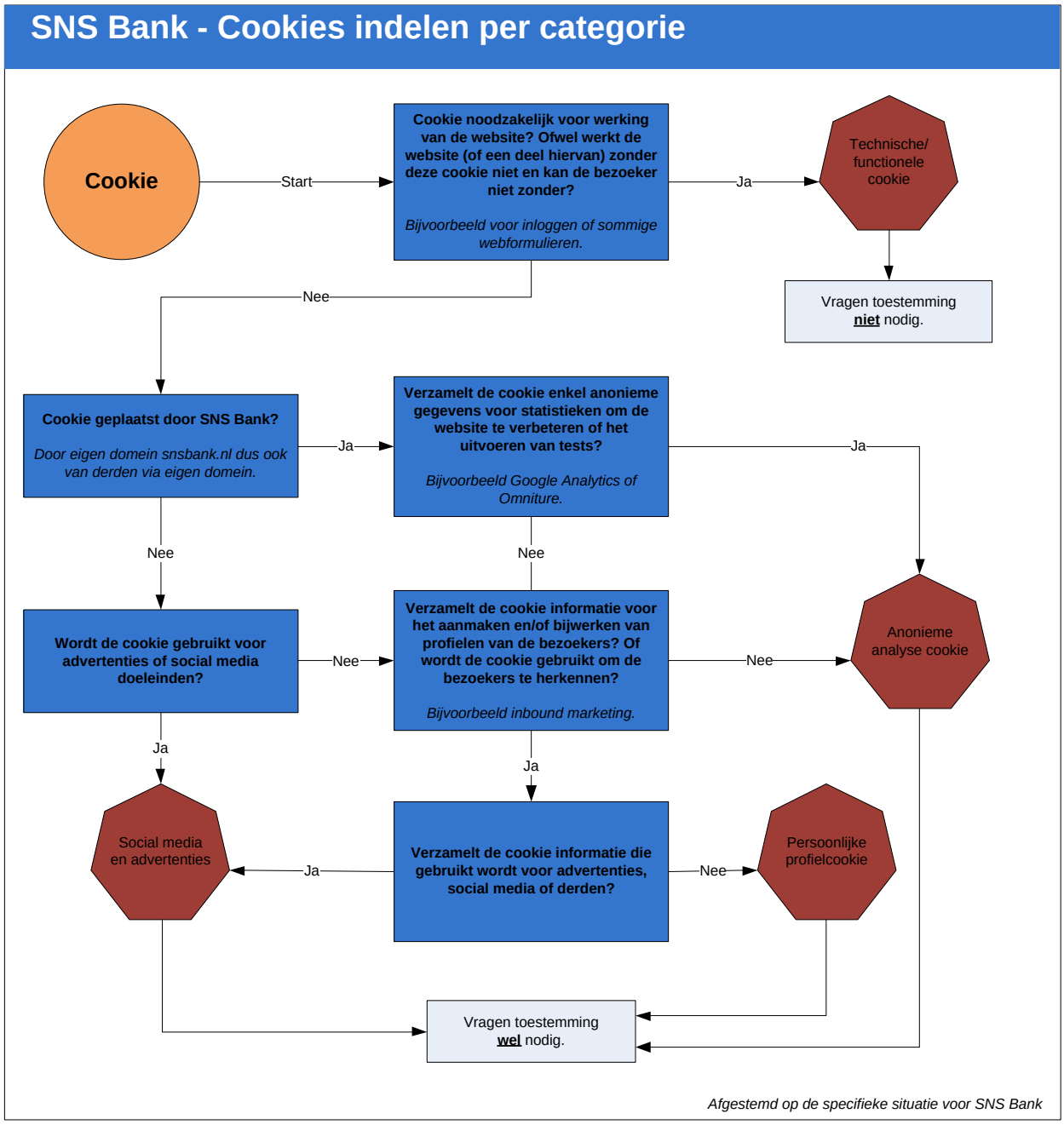
8.1 Details Cookies

Lijst met website pagina's waarvan de cookies en bijbehorende eigenschappen onderzocht zijn.

Nr.	URL
1	http://www.snsbank.nl/particulier/home.html
2	http://www.snsbank.nl/particulier/sparen.html
3	http://www.snsbank.nl/zakelijk/home.html
4	https://www.snsbank.nl/mijnsns/secure/loginzakelijk.html
5	http://www.snsbank.nl/particulier/hypotheek/hypotheken-1.html
6	http://www.snsbank.nl/particulier/hypotheek/sns-bank-maakt-aflossen-betaalbaar.html
7	https://www.snsbank.nl/particulier/betalen/sns-betalen/sns-betalen-openen/bedankt-voor-je-aanvraag.html?testmode=yes
8	https://banksparen.snsbank.nl/goudenhanddruk/stap1/default.aspx
9	https://lenen.snsbank.nl/alternatief.aspx
10	https://forum.snsbank.nl/invitation.php?referer=http%3A%2F%2Fforum.snsbank.nl%2Fshowthread.php%3Ft%3D6793%26p%3D46919
11	http://www.snsbank.nl/particulier/pensioen/afspraak-maken-gouden-handdruk/bedankt.html
12	http://www.snsbank.nl/index.asp?navigationID=9212
13	https://www.snsbank.nl/particulier/wachtwoord-vergeten.html
14	http://www.snsbank.nl/particulier/hypotheek/sns-bank-maakt-aflossen-betaalbaar.html
15	https://www.snsbank.nl/particulier/betalen/klantenservice/rood-staan-2/rood-staan-op-je-betaalrekening.html
16	http://www.snsbank.nl/zakelijk/zakelijk-betalen.html
17	https://www.snsbank.nl/particulier/klantenservice/faq-zoekresultaten.html?Qgo_REF=sns_part&maxResults=7&searchphrase=cookies
18	https://www.snsbank.nl/particulier/klantenservice/mijn-sns/bankieren-met-je-mobiel.html
19	https://forum.snsbank.nl/showthread.php?t=6826
20	http://www.snsbank.nl/particulier/sparen/je-sns-spaarrekening-openen.html?adtype=SEA.Branding.-Sns%20bank-Branding_SNSBank&adrecip=google&adwcmp=gooppc_s!53426315!1903077395!13397277635!sns%20bank!e

Verdere details alleen beschikbaar binnen SNS Bank.

8.2 Cookies indelen



8.3 Requirements

Nr	Naam	Beschrijving	Relatie	Prioriteit	Opmerking
1	Bezoeker informeren op de website	De bezoeker dient bij het bezoeken van de website gelijk geïnformeerd te worden over welke categorieën cookies geplaatst worden en waarvoor deze gebruikt worden.		Must	Informeren is fase 1.
2	Privacy statement wijzigen	Het privacy statement dient gewijzigd te worden zodat het informeren en toestemming vragen op de website begrijpbaar en juridisch beschreven zijn.	1	Must	
3	Basis informatie omtrent cookies	Op de website dient er basis informatie over de cookies en hun details beschikbaar te zijn wanneer de bezoeker om toestemming wordt gevraagd.	1	Must	
4	Volledige informatie omtrent cookies	Op de website dient er na doorklikken volledige informatie (zoals gesteld in de wetgeving) over de cookies en hun eigenschappen beschikbaar te zijn wanneer de bezoeker om toestemming wordt gevraagd.	1,3	Must	
5	Informatie altijd bereikbaar	Altijd dient de informatiepagina met (basis en volledige) informatie over cookies en toestemming te bereiken zijn.	3,4	Must	
6	Toestemming vragen aan de bezoeker	Bij een bezoek aan de website dient de bezoeker geïnformeerd te worden over het gebruik van cookies en zijn niveau van toestemming kunnen kiezen.	1	Must	Toestemming vragen en verwerken is fase 2.
7	Geen toestemming voor cookies	De bezoeker kan ervoor kiezen om geen toestemming te verlenen voor iedere categorie cookies.	6	Must	Geen toestemming impliceert dat technische cookies wel geplaatst en gebruikt

					worden.
8	Toestemming voor alle cookies	De bezoeker kan ervoor kiezen toestemming te verlenen voor alle categorieën cookies (te weten: Anonieme analysecookies, Persoonlijke profielcookies, Social Media en advertenties).	6	Must	
9	Toestemming voor categorieën cookies	De bezoeker kan toestemming verlenen voor bepaalde categorieën cookies (te weten: Anonieme analysecookies, Persoonlijke profielcookies, Social Media en advertenties) in oplopende volgorde.	6	Must	Samenhang tussen categorieën: Bij Social Media en advertenties, ook Anonieme analysecookies en Persoonlijke profielcookies. Bij Persoonlijke profielcookies, ook Anonieme analysecookies. Of alleen Anonieme analysecookies.
10	Toestemming vragen op iedere pagina	Altijd als er een bezoeker op de website komt die nog geen keuze voor toestemming (opt-in) heeft gemaakt, dient er toestemming gevraagd te worden. De toestemming wordt gevraagd ongeacht op welke pagina de bezoeker binnenkomt.	6	Must	
11	Toestemming opslaan in cookie	Het niveau van de toestemming van de bezoeker dient vastgelegd te worden in een cookie op de randapparatuur van de bezoeker, opgeslagen dient te worden: een unieke code, toestemming voor welke categorie(n) en het tijdstip om zo te kunnen bewijzen dat de toestemming is verleend.	6	Must	

12	Toestemming opslaan in database	Het niveau van de toestemming van de bezoeker dient vastgelegd te worden in een database, opgeslagen dient te worden: een unieke code, toestemming voor welke categorie(n) en het tijdstip om zo te kunnen bewijzen dat de toestemming is verleend.	6	Should	
13	Toestemming controleren	Bij een bezoek aan de website wordt gecontroleerd of de bezoeker toestemming heeft verleend en zo ja, het niveau van toestemming voor welke categorie(n) cookies.	11,12	Must	
14	Toestemming verwerken	Bij een bezoek aan de website worden alleen de categorie(n) cookies geplaatst waarvoor door de bezoeker eerder toestemming is gegeven.	11,12	Must	
15	Toestemming wijzigen op website	Wanneer een bezoeker bezoekt moet hij zijn toestemming kunnen inzien, intrekken en wijzigen.	6,11,12	Must	Dit kan via hetzelfde scherm als bij 'Toestemming vragen aan de bezoeker'.
16	Toestemming wijzigen in inlogomgeving	Wanneer een bezoeker ingelogd is op de inlogomgeving moet de bezoeker zijn toestemming kunnen inzien, intrekken en wijzigen.	6,11,12	Should	Hiervoor kan een andere manier gehanteerd worden dan op de website.
17	Toestemming verkrijgen voor meer cookies	Wanneer een bezoeker op pagina's is waar een formulier ingevuld kan worden of een mogelijkheid met social media is, dient de optie om toestemming (voor meer categorieën cookies) te geven duidelijk zichtbaar te zijn om zo transparant te zijn en meer toestemming te verkrijgen.	6	Should	

18	Toestemming verkrijgen voor minder cookies	Wanneer een bezoeker zijn toestemming intrekt of voor minder cookies toestemming geeft dienen de geplaatste cookies op de randapparatuur van de bezoeker niet meer gebruikt te worden.	6	Must	
19	Wijzigen van scherm	Het scherm waarin toestemming gevraagd wordt en de pagina waar de informatie te vinden is dient aanpasbaar te zijn vanuit het Content Management System.	1,3,4,6	Should	De gewijzigde wetgeving en uitwerking kan nog veranderen aangezien het onbekend is, wijzigingen kunnen doorvoeren moet daarom mogelijk zijn.
20	Consequentie van niet plaatsen cookie	Wanneer een cookie niet geplaatst wordt kan dit consequenties hebben voor de werking van de website, dit dient opgevangen (alternatieven) en geregistreerd te worden.		Must	
21	Alternatieven voor plaatsen cookies	Het gebruik van alternatieven voor cookies (Cookie-less script), zoals het plaatsen van scripts moet mogelijk zijn vanuit het Content Management System.		Must	
22	Cookies externe websites	Voor externe websites dient het informeren en toestemming vragen/verwerken ook gerealiseerd te worden vanwege de wetgeving.	6,11,12	Should	
23	Cookies mobiel	Voor mobiel (Apps) dient het informeren en toestemming vragen/verwerken ook gerealiseerd te worden vanwege de wetgeving.	6,11,12	Should	
24	Cookies per online applicatie	Per online applicatie op de website in kaart brengen welke cookies gebruikt worden en tot welke categorie deze behoren.		Must	

25	Cookies in content	Voor alle content in kaart brengen welke cookies gebruikt worden en tot welke categorie deze behoren.		Must	
26	Beheer geprogrammeerde cookies	Geprogrammeerde cookies op de website ('Harde cookies') inzichtelijk maken en centraal beheer inrichten in de vorm van een generieke oplossing voor plaatsing.		Must	Overzicht creëren en zodoende de beheerbaarheid van cookies te kunnen realiseren.
27	Beheer weergave overzicht cookies	Het overzicht van alle cookies kan vaak veranderen dus deze dient snel aanpasbaar te zijn in het Content Management System.	23-27	Must	
28	Cookies verbinden aan categorieën	Iedere cookie die geplaatst wordt bij bezoek aan de website dient verbonden te worden aan de categorie van toestemming.	7,8,9,28	Must	Soort label wat aangeeft of de cookie geplaatst mag worden bij toestemming voor categorie cookies.
29	Testen van opties	Het dient mogelijk te zijn om AB tests uit te voeren om zodoende te kunnen onderzoeken welke optie voor toestemming vragen beter is.	1,3,4,6	Must	Tests uitvoeren zonder gebruik van cookies.
30	Analyse gegevens van tests	Analyse gegevens voor inzicht in de categorieën waarvoor bezoekers toestemming verlenen moeten beschikbaar zijn.	30	Must	
31	Aantonen toestemming (bewijslast)	Altijd dient de toestemming van een bezoeker aangetoond te kunnen worden (bewijslast).	11,12	Must	
32	Verwerking informatie inzichtelijk maken	De wetgeving vereist dat het verwerkingsproces van informatie door middel van cookies inzichtelijk is en duidelijk aan te tonen is dat de privacy van de bezoeker gerespecteerd wordt.	11,12	Must	In beginsel vallen cookies onder de Wbp, dit wordt aangeduid als de omgekeerde bewijslast.
33	Technische cookies altijd plaatsen	Ongeacht voor welke categorie cookies de bezoeker toestemming geeft worden technische cookies altijd geplaatst.		Must	

34	Bezoeker kan website altijd bezoeken	De website is voor een bezoeker altijd te bezoeken ongeacht het niveau van toestemming.		Must
35	Website drempelvrij	De website zal drempelvrij blijven voor de bezoeker en hiermee voldoen aan de eisen van het Waarmerk Drempelvrij	1,3,4,6	Must

Dit is een overzicht met minder details, de volledige versie is alleen binnen SNS Bank beschikbaar. Dit betreffen requirements voor een mogelijke oplossing.